

THE HONORABLE RICHARD A. JONES

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STEVEN VANCE, *et al.*,

v.

AMAZON.COM, INC.,

Plaintiffs,

Defendant.

No. 2:20-cv-01084-RAJ

DEFENDANT AMAZON.COM,
INC.'S MOTION TO DISMISS

NOTE ON MOTION CALENDAR:
OCTOBER 9, 2020

ORAL ARGUMENT REQUESTED

TABLE OF CONTENTS

	Page
AMAZON HAS CONFERRED WITH PLAINTIFFS.....	3
FACTUAL BACKGROUND.....	3
A. The Illinois Biometric Information Privacy Act.	3
B. The DiF Dataset.	4
C. Amazon’s Alleged Conduct.	6
ARGUMENT.....	6
I. THE COURT SHOULD DISMISS PLAINTIFFS’ BIPA CLAIMS.	7
A. Plaintiffs Do Not Allege Any Asserted Violations Occurred “Primarily and Substantially” in Illinois, as Required to State a BIPA Claim.	7
B. Plaintiffs’ BIPA Claims Violate the Dormant Commerce Clause.....	9
1. Plaintiffs’ Claims Impermissibly Attempt to Regulate Conduct Occurring Entirely Outside of Illinois’s Borders.....	9
2. Plaintiffs’ BIPA Claims Impermissibly Displace the Legislation and Policy Decisions Made by States Other than Illinois.....	12
C. Plaintiffs Fail to State a Claim Under BIPA Sections 15(b) Or 15(c).	16
1. BIPA Does Not Apply to the Use of Photographs.....	16
2. Plaintiffs Cannot State a Section 15(b) Claim Because they Fail to Adequately Allege that Amazon “Collected” or “Otherwise Obtained” Their Biometrics.	18
3. Plaintiffs Cannot Plead a Section 15(c) Claim because they Fail to Plausibly Allege that Amazon “Profited” from Their Biometrics.	21
II. THE COURT SHOULD DISMISS PLAINTIFFS’ UNJUST ENRICHMENT CLAIM.....	21
III. PLAINTIFFS HAVE NO SEPARATE INJUNCTIVE RELIEF CLAIM.	23
CONCLUSION.....	23

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>ACLU v. Johnson</i> , 194 F.3d 1149 (10th Cir. 1999)	15
<i>Aisha Namuwonge v. Kronos, Inc.</i> , 418 F. Supp. 3d 279 (N.D. Ill. 2019)	19
<i>Am. Booksellers Found. v. Dean</i> , 342 F.3d 96 (2d Cir. 2003).....	15
<i>Am. Libraries Ass’n v. Pataki</i> , 969 F. Supp. 160 (S.D.N.Y. 1997)	15
<i>Archdiocese of St. Louis v. Internet Entm’t Grp., Inc.</i> , 1999 WL 66022 (E.D. Mo. Feb. 12, 1999).....	15
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	6
<i>Avery v. State Farm Mut. Auto. Ins. Co.</i> , 835 N.E.2d 801 (Ill. 2005)	7, 9
<i>Backpage.com, LLC v. McKenna</i> , 881 F. Supp. 2d 1262 (W.D. Wash. 2012).....	15
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	6
<i>Bernal v. ADP, LLC</i> , No. 2017-CH-12364, Order (Cook Cty. Ill. Cir. Ct. Aug. 23, 2019).....	19, 20
<i>Cameron v. Polar Tech Indus., Inc. & ADP, LLC</i> , No. 2019-CH-000013 (DeKalb Cty. Ill. Cir. Ct. Aug. 23, 2019)	19
<i>Chinatown Neighborhood Ass’n v. Harris</i> , 794 F.3d 1136 (9th Cir. 2015)	10
<i>Cleary v. Philip Morris Inc.</i> , 656 F.3d 511 (7th Cir. 2011)	21
<i>Cousineau v. Microsoft Corp.</i> , 992 F. Supp. 2d 1116 (W.D. Wash. 2012).....	21, 22
<i>In re D.W.</i> , 827 N.E.2d 466 (Ill. 2005).....	19

1	<i>Dana Tank Container, Inc. v. Human Rights Comm’n</i> ,	
	687 N.E.2d 102 (Ill. App. Ct. 1997)	19
2	<i>Daniels Sharpsmart, Inc. v. Smith</i> ,	
3	889 F.3d 608 (9th Cir. 2018)	10
4	<i>Edifecs Inc., v. TIBCO Software Inc.</i> ,	
5	2011 WL 1045645 (W.D. Wash. Mar. 23, 2011)	23
6	<i>Edwards v. JPMorgan Chase Bank, N.A.</i> ,	
	2011 WL 3516155 (W.D. Wash. Aug. 11, 2011)	23
7	<i>In re Facebook Biometric Information Privacy Litigation</i> ,	
8	185 F. Supp. 3d 1155 (N.D. Cal. 2016)	17, 18
9	<i>Healy v. Beer Inst., Inc.</i> ,	
10	491 U.S. 324 (1989)	2, 9, 12
11	<i>Heard v. Becton, Dickinson & Co.</i> ,	
	440 F. Supp. 3d 960 (N.D. Ill. 2020)	19
12	<i>Kelley v. Microsoft Corp.</i> ,	
13	251 F.R.D. 544 (W.D. Wash. 2008)	22
14	<i>L’Garde, Inc. v. Raytheon Space & Airborne Sys.</i> ,	
15	805 F. Supp. 2d 932 (C.D. Cal. 2011)	5
16	<i>Landau v. CNA Fin. Corp.</i> ,	
	886 N.E.2d 405 (Ill. App. 2008)	7
17	<i>Monroy v. Shutterfly, Inc.</i> ,	
18	2017 WL 4099846 (N.D. Ill. Sept. 15, 2017)	7, 8, 11, 18
19	<i>Mount v. PulsePoint, Inc.</i> ,	
20	684 Fed. App’x 32 (2d Cir. 2017), as amended (May 3, 2017)	22
21	<i>Nat’l Collegiate Athletic Ass’n v. Miller</i> ,	
	10 F.3d 633 (9th Cir. 1993)	13, 14
22	<i>Nat’l Solid Wastes Mgmt. Ass’n v. Meyer</i> ,	
23	63 F.3d 652 (7th Cir. 1995)	13
24	<i>Neals v. PAR Tech. Corp.</i> ,	
25	419 F. Supp. 3d 1088 (N.D. Ill. 2019)	9
26	<i>Patel v. Facebook, Inc.</i> ,	
	932 F.3d 1264 (9th Cir. 2019)	7, 8, 18

1	<i>Pooh-Bah Enter., Inc. v. Cnty. of Cook,</i>	
	905 N.E.2d 781 (Ill. 2009)	21
2	<i>Reyn's Pasta Bella, LLC v. Visa USA, Inc.,</i>	
3	442 F.3d 741 (9th Cir. 2006)	5
4	<i>Rivera v. Google, Inc.,</i>	
5	238 F. Supp. 3d 1088 (N.D. Ill. 2017)	7, 8, 18
6	<i>Rosenbach v. Six Flags Entm't Corp.,</i>	
	129 N.E.3d 1197 (Ill. 2019)	18
7	<i>Sam Francis Found. v. Christies, Inc.,</i>	
8	784 F.3d 1320 (9th Cir. 2015)	10, 11
9	<i>Seattle Prof'l Eng'g Employees Ass'n v. Boeing Co.,</i>	
10	139 Wn.2d 824, 991 P.2d 1126 (2000)	23
11	<i>Tarzian v. Kraft Heinz Foods Co.,</i>	
	2019 WL 5064732 (N.D. Ill. Oct. 9, 2019)	9
12	<i>Vance et al. v. Microsoft Corp.,</i>	
13	W.D. Wash. No. 2:20-cv-01082-JCC-MAT	1
14	<i>Welborn v. Internal Revenue Serv.,</i>	
15	218 F. Supp. 3d 64 (D.D.C. 2016)	22
16	State Statutes	
	740 ILCS	
17	14 (Illinois Biometric Information Privacy Act)	<i>passim</i>
18	14/5	18
19	14/5(a)	3
	14/5(b)	3
20	14/5(b)-(e)	18
	14/5(d)	4
21	14/5(e)	4
	14/10	4, 16
22	14/15	19
	14/15(a)	19
23	14/15(b)	<i>passim</i>
	14/15(c)	<i>passim</i>
24	14/15(d)	19
	14/15(e)	19
25	14/20(2)	4
26		

RCW

19.375.010(1).....	12, 13
19.375.010(4).....	12, 13
19.375.010(5).....	13
19.375.020.....	13
19.375.020(1).....	12
Chapter 49.52.....	23

Rules

Federal Rule of Civil Procedure 12(b)(6)	<i>passim</i>
--	---------------

Constitutional Provisions

U.S. Constitution, Article I, section 8	9
---	---

Other Authorities

Ira Kemelmacher-Shlizerman et al., <i>The MegaFace Benchmark: 1 Million Faces for Recognition at Scale</i> , UNIVERSITY OF WASHINGTON (2015)	15
--	----

New York State, <i>Department of State, Division of Corporations, State Records & UCC, Search The Corporation and Business Entity Database Results for International Business Machines Corporation, https://www.dos.ny.gov/corps/bus_entity_search.html</i> (last accessed Sept. 10, 2020)	5
--	---

Oxford English Dictionary (Mar. 2006), <i>available at https://www.oed.com/view/Entry/142818?rskey=8jt7S7&result=1&isAdvanced=false#eid</i>	18
--	----

Sen. Bill 2400,	
§ 10 (Feb. 14, 2008)	16
§ 10 (Apr. 11, 2008)	17
§ 10 (May 28, 2008)	17

State of Delaware, <i>Department of State: Division of Corporations, Business Search Results for Oath Inc., https://icis.corp.delaware.gov/ecorp/entitysearch/NameSearch.aspx</i> (last accessed Sept. 10, 2020)	5
--	---

Webster's Dictionary 373 (2008 ed.)	18
---	----

1 Illinois residents Steven Vance and Tim Janecyk allege that Amazon¹ is liable for
 2 violating the Illinois Biometric Information Privacy Act (“BIPA”) by downloading an IBM-
 3 created dataset consisting of one million facial images, known as the Diversity in Faces
 4 Dataset (the “DiF Dataset”), which was created in 2019 “for the purpose of improving the
 5 ability of facial recognition systems to fairly and accurately identify all individuals.” Dkt. 1,
 6 Compl. ¶ 42. Plaintiffs seek to hold Amazon liable for penalties under BIPA, even though
 7 they allege that *IBM*—not Amazon—included their images and biometric information in the
 8 DiF Dataset.

9 Plaintiffs allege that they voluntarily uploaded their photographs many years ago to
 10 Flickr, a photo-sharing website. They further allege that Flickr then made their images
 11 publicly available in a collection of 100 million photographs, from which IBM culled one
 12 million images to create the DiF Dataset. Plaintiffs do *not* allege that Amazon (i) interacted
 13 with Plaintiffs or any other Flickr users who were Illinois residents, (ii) conducted any activity
 14 relevant to this lawsuit in Illinois, (iii) ever linked Plaintiffs’ identities with their individual
 15 biometric information, or (iv) ever engaged in any transactions to profit from Plaintiffs’ data.
 16 Nevertheless, Plaintiffs contend that Amazon’s out-of-state conduct was regulated by BIPA
 17 and that Amazon violated BIPA by “collecting and obtaining individuals’ biometric
 18 identifiers and information ... without providing the requisite written information and without
 19 obtaining the requisite written releases.” Dkt. 1, Compl. ¶ 100. Plaintiffs seek to represent a
 20 class of any other Illinois residents whose images appear in the DiF Dataset.

21
 22
 23
 24 ¹ Plaintiffs Vance and Janecyk, represented by the same counsel, are pursuing a substantially
 25 identical putative class action against Microsoft, claiming BIPA violations based on
 26 allegations that, like Amazon, Microsoft downloaded the Diversity in Faces Dataset from
 IBM. *See Vance et al. v. Microsoft Corp.*, W.D. Wash. No. 2:20-cv-01082-JCC-
 MAT. Amazon understands Microsoft is likewise filing a motion to dismiss the claims
 against it, asserting the same dismissal arguments Amazon asserts in this Motion.

1 Plaintiffs fail to state a viable claim. The Court should dismiss Plaintiffs' four-count
 2 Complaint, under Federal Rule of Civil Procedure 12(b)(6), with prejudice for the following
 3 reasons:

4 *First*, the BIPA claims (Counts I and II) fail because Illinois statutes do not have
 5 extraterritorial effect unless a clear intent to the contrary appears in the statute. Because
 6 BIPA conveys no such intent for extraterritorial application, the statute could regulate
 7 Amazon only if its BIPA-related conduct occurred primarily and substantially in Illinois. But
 8 Plaintiffs fail to allege that Amazon engaged in *any* conduct in Illinois giving rise to BIPA
 9 liability. Plaintiffs allege only that the DiF Dataset, which Amazon obtained from IBM,
 10 included publicly-available online photographs of Vance and Janecyk, who are allegedly
 11 Illinois residents. BIPA does not reach Amazon's alleged conduct.

12 *Second*, applying BIPA to Amazon's out-of-state conduct would violate the dormant
 13 Commerce Clause, which "precludes the application of a state statute" that has "the practical
 14 effect of ... control[ing] conduct beyond the boundaries of the State, ... whether or not the
 15 commerce has effects within the State." *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336 n.1
 16 (1989). If Plaintiffs' allegations could support a BIPA claim, it would mean that a business in
 17 Washington could not engage in an online transaction with a business in New York without
 18 subjecting itself to penalties in Illinois—even if it does nothing in Illinois relating to the
 19 transaction and even if Washington law is to the contrary. That is not the law.

20 *Third*, even if BIPA applied, Plaintiffs fail to state a claim under BIPA's plain
 21 language. Neither Section 15(b) nor Section 15(c) of BIPA applies to information derived
 22 from "photographs." Section 15(b) also does not create a cause of action for mere passive
 23 possession of biometric identifiers or information by third parties. And Plaintiffs fail to
 24 plausibly plead that Amazon "profited" from Plaintiffs' biometric identifiers or information
 25 and thus fail to state a Section 15(c) claim.
 26

1 *Fourth*, Plaintiffs fail to state an unjust enrichment claim (Count III) because they fail
 2 plausibly to allege that (i) Amazon was enriched by their biometric identifiers or biometric
 3 information; (ii) they suffered any expense or loss; or (iii) they lack an adequate remedy at
 4 law, because the alleged BIPA violations are the only basis for the unjust enrichment claim.

5 *Fifth*, Plaintiff's "injunctive relief" claim (Count IV) is merely a prayer for a form of
 6 relief, not a claim.

7 **AMAZON HAS CONFERRED WITH PLAINTIFFS**

8 Pursuant to the Court's Standing Order for Civil Cases (Dkt. 2, ¶ 6), counsel for
 9 Amazon conferred with Plaintiffs' counsel regarding the subject of this Motion, and the
 10 parties were unable to agree on a resolution. Decl. of Jaime Drozd Allen ("Allen Decl."), ¶ 2–
 11 5. Plaintiffs contend that their BIPA claims do not violate Illinois's extraterritoriality doctrine
 12 or the dormant Commerce Clause, that BIPA applies to Amazon's alleged analysis of photos,
 13 and that Plaintiffs adequately allege claims under BIPA Sections 15(b) and 15(c) and for
 14 unjust enrichment. *See id.* ¶ 4. Amazon disputes Plaintiffs' positions and maintains that the
 15 Complaint should be dismissed under Rule 12(b)(6) for the reasons stated below.

16 **FACTUAL BACKGROUND**

17 **A. The Illinois Biometric Information Privacy Act.**

18 In 2008, the Illinois General Assembly enacted BIPA to address the growing use of
 19 biometric technology "in the business and security screening sectors" in Illinois. 740 ILCS
 20 14/5(a). The General Assembly found that "[m]ajor national corporations ha[d] selected the
 21 City of Chicago and other locations in [Illinois] as pilot testing sites for new applications of
 22 biometric-facilitated financial transactions, including finger-scan technologies at grocery
 23 stores, gas stations, and school cafeterias." 740 ILCS 14/5(b). The Illinois legislature also
 24 found that consumers had concerns about "the use of biometrics when such information is tied
 25 to finances" and were "deterred from partaking in biometric identifier-facilitated
 26 transactions," in part because of the "limited State law regulating the collection, use,

1 safeguarding, and storage of biometrics.” 740 ILCS 14/5(d), (e). BIPA addresses these
 2 concerns by regulating the collection, possession, and storage of certain biometric identifiers
 3 and information, while expressly excluding coverage of other data.

4 The statute defines “biometric identifier” using a short, exclusive list of sources of
 5 personal data: “[b]iometric identifier” means a retina or iris scan, fingerprint, voiceprint, or
 6 scan of hand or face geometry.” 740 ILCS 14/10. BIPA Section 15(b) requires private
 7 entities that “collect, capture, purchase, receive through trade, or otherwise obtain a person’s
 8 ... biometric identifier or biometric information” to first (1) inform the person of that
 9 collection “in writing”; (2) inform the person “in writing of the specific purpose and length of
 10 term” regarding the collection; and (3) obtain a “written release” from the person. 740 ILCS
 11 14/15(b). BIPA Section 15(c) further prohibits any private entity “in possession of a
 12 biometric identifier or biometric information” from “sell[ing], leas[ing], trad[ing], or
 13 otherwise profit[ing] from a person’s ... biometric identifier or biometric information.” 740
 14 ILCS 14/15(c).

15 For negligent violations of BIPA, a plaintiff can obtain “liquidated damages of \$1,000
 16 or actual damages, whichever is greater,” and for intentional or reckless violations of BIPA, a
 17 plaintiff can collect “liquidated damages of \$5,000 or actual damages, whichever is greater.”
 18 740 ILCS 14/20(2).

19 **B. The DiF Dataset.**

20 Plaintiffs Steven Vance and Tim Janecyk allege that, in 2008 and 2011, respectively,
 21 they uploaded photos of themselves to the photo-sharing website Flickr. Compl. ¶¶ 66, 75.
 22 Each alleges they performed their uploads using devices in Illinois. *Id.* Plaintiffs contend
 23 that, in 2014, Yahoo!—Flickr’s parent company at the time—released to the public
 24 approximately 100 million photos uploaded by Flickr users (the “Flickr Dataset”). *Id.* ¶ 29.
 25 Oath Inc.—the current name of the entity formerly known as Yahoo!—is a Delaware
 26 corporation headquartered in Sunnyvale, California. *See* State of Delaware, *Department of*

1 *State: Division of Corporations, Business Search Results for Oath Inc.*,
 2 <https://icis.corp.delaware.gov/ecorp/entitysearch/NameSearch.aspx> (last accessed Sept. 10,
 3 2020); *see also Reyn's Pasta Bella, LLC v. Visa USA, Inc.*, 442 F.3d 741, 746, n.6 (9th Cir.
 4 2006) (the Court may take judicial notice of information posted on a state government is
 5 "readily verifiable and, therefore, the proper subject of judicial notice."); *L'Garde, Inc. v.*
 6 *Raytheon Space & Airborne Sys.*, 805 F. Supp. 2d 932, 938 (C.D. Cal. 2011) (taking judicial
 7 notice of "Business Entity Detail" search result from Secretary of State website submitted in
 8 support of motion to dismiss). Plaintiffs do not allege any interaction or relationship between
 9 Flickr and Amazon.

10 Plaintiffs next assert that, in 2019, New York-based International Business Machines
 11 Corporation ("IBM") created "a new dataset consisting of one million images culled from the
 12 Flickr Dataset ... for the purpose of improving the ability of facial recognition systems to
 13 fairly and accurately identify all individuals" (the "Diversity in Faces Dataset" or "DiF
 14 Dataset"). Compl. ¶ 42. Plaintiffs contend that IBM included their photos in the DiF Dataset,
 15 and that in creating the Dataset, IBM "scanned the facial geometry of each image contained in
 16 the dataset" and created "biometric identifiers" and "biometric information." Compl. ¶¶ 43,
 17 46. According to Plaintiffs, the DiF dataset included a "comprehensive set of annotations of
 18 intrinsic facial features that includes craniofacial distances, areas and ratios, facial symmetry
 19 and contrast, skin color, age and gender predictions, subjective annotations, and pose and
 20 resolution." *Id.* ¶ 43 (citation omitted).

21 IBM is a New York corporation with its headquarters in New York, New York. *See*
 22 *New York State, Department of State, Division of Corporations, State Records & UCC,*
 23 *Search The Corporation and Business Entity Database Results for International Business*
 24 *Machines Corporation*, https://www.dos.ny.gov/corps/bus_entity_search.html (last accessed
 25 Sept. 10, 2020). Plaintiffs do not allege that IBM engaged in this conduct in Illinois or that
 26 IBM knew the culled images included photographs of Illinois residents. Nevertheless, they

1 claim that BIPA regulates the purported “biometric identifiers” and “biometric information”
 2 that IBM allegedly created from the Flickr photographs. *See* Compl. ¶ 46. Plaintiffs further
 3 claim that IBM made the DiF Dataset available to other companies. *Id.* ¶ 49.

4 C. Amazon’s Alleged Conduct.

5 Plaintiffs assert that Amazon “applied for and obtained the Diversity in Faces Dataset
 6 from IBM.” *Id.* ¶ 61. Plaintiffs do *not* allege that Amazon’s acquisition of the DiF Dataset
 7 had any connection whatsoever with Illinois. For example, Plaintiffs do not claim they
 8 personally uploaded photos to Amazon servers, used Amazon software, services, or
 9 technology, or ever communicated or interacted with Amazon. Nor do Plaintiffs allege that
 10 any of Amazon’s alleged actions in purported violation of BIPA—e.g., “collecting, capturing
 11 and otherwise obtaining the[ir] biometric identifiers and information” and/or “profit[ing]”
 12 from that data, *id.* ¶¶ 65, 71–72, 79–80, 107—took place in Illinois. Amazon’s only alleged
 13 connection to Illinois is allegedly possessing IBM’s DiF Dataset of publicly-available photos
 14 of approximately one million individuals, some undetermined number of which allegedly
 15 include Illinois residents. *See id.* ¶¶ 69, 77.

16 ARGUMENT

17 Rule 12(b)(6) requires dismissal when a plaintiff “fail[s] to state a claim upon which
 18 relief can be granted.” Fed. R. Civ. P. 12(b)(6). To plead a viable cause of action, the
 19 allegations must transcend the “speculative,” “conceivable,” and “possible” and “state a claim
 20 that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555–57, 566–67, 570
 21 (2007). The Court must disregard “legal conclusions” and “conclusory statements” and must
 22 scrutinize factual allegations to ensure that they are more than “merely consistent with a
 23 defendant’s liability.” *Ashcroft v. Iqbal*, 556 U.S. 662, 677–79 (2009). Plaintiffs fail to state
 24 a claim, and this Court should dismiss the Complaint with prejudice.

I. THE COURT SHOULD DISMISS PLAINTIFFS' BIPA CLAIMS.

A. Plaintiffs Do Not Allege Any Asserted Violations Occurred “Primarily and Substantially” in Illinois, as Required to State a BIPA Claim.

Under Illinois law, “a statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute.” *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 852 (Ill. 2005) (citation omitted). “[N]one of BIPA’s express provisions indicates that the statute was intended to have extraterritorial effect.” *Monroy v. Shutterfly, Inc.*, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017). Because BIPA “was not intended to and does not have extraterritorial application,” “asserted violations of [BIPA] must have taken place in Illinois.” *Rivera v. Google, Inc.*, 238 F. Supp. 3d 1088, 1100, 1104 (N.D. Ill. 2017). This requires an assessment “as to where the essential elements of a BIPA violation take place.” *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1276 (9th Cir. 2019). Accordingly, Amazon could be subject to BIPA only if “the majority of circumstances relating to the alleged violation of the [statute]” occurred in Illinois. *Landau v. CNA Fin. Corp.*, 886 N.E.2d 405, 409 (Ill. App. 2008). Put another way, Amazon could be subject to BIPA only “if the circumstances relating to the claim occur[ed] primarily and substantially” in Illinois. *Avery*, 835 N.E.2d at 854; *see also Patel*, 932 F.3d at 1275–76 (applying “primarily and substantially” test to BIPA claim). Plaintiffs’ claims fail this basic test.

For Plaintiffs’ Section 15(b) claim, Plaintiffs would have to prove Amazon’s alleged “collection” of Plaintiffs’ biometric data from IBM was without prior notice to Plaintiffs (who were, of course, unknown to Amazon before the filing of this lawsuit) and without their written consent. *See* Compl. ¶ 100; 740 ILCS 14/15(b). For Plaintiffs’ Section 15(c) claim, Plaintiffs would have to prove Amazon “profited” from Plaintiffs’ biometric data. *See* Compl. ¶ 107; 740 ILCS 14/15(c). Plaintiffs do not sufficiently allege Amazon engaged in any of this conduct in Illinois—and nor could they in good faith.

1 Amazon's alleged possession of photographs of Illinois residents, Compl. ¶¶ 69, 77,
 2 even if true, would **not** show that Amazon collected biometric data or profited from that data
 3 in Illinois. On the contrary, Plaintiffs allege that Amazon obtained the DiF Dataset online
 4 from IBM (a New York corporation) for free. Compl. ¶¶ 51, 61–62. Plaintiffs fail to allege
 5 that this non-commercial transaction occurred “primarily and substantially” in Illinois, nor
 6 could they.

7 Plaintiffs also allege that Amazon “developed, produced, marketed and otherwise used
 8 facial recognition products and technologies in connection with its business,” and that
 9 “Amazon’s core facial recognition product is Amazon Rekognition,” which Plaintiffs describe
 10 as “a fundamental cornerstone of many of Amazon’s largest consumer products and services
 11 around the world.” *Id.* ¶¶ 55–56. Plaintiffs further allege, “[o]n information and belief,” that
 12 “Amazon has also profited from selling its facial recognition technology to third parties.” *Id.*
 13 ¶ 56. But Plaintiffs’ conclusory allegations do not plausibly explain how these activities have
 14 any connection to the DiF Dataset. In particular, Plaintiffs fail to allege how the DiF Dataset,
 15 released in 2019, played any role in Amazon’s development of any facial-recognition
 16 products sold in Illinois, let alone that photographs **from Illinois residents** specifically were
 17 used in that development.

18 While a few courts have found it premature at the motion to dismiss stage to determine
 19 whether a plaintiff’s claims would require an extraterritorial application of BIPA, those cases
 20 are distinguishable in an important respect: in each case, an Illinois plaintiff allegedly
 21 uploaded a photo **directly** to the **defendant’s** systems from a computer or device located in
 22 Illinois, so the defendant’s collection arguably occurred in Illinois. *See, e.g., Patel*, 932 F.3d
 23 at 1268, 1276 (Illinois-based Facebook users uploaded their photos to Facebook from
 24 Illinois); *Monroy*, 2017 WL 4099846, at *6 (plaintiff “allege[d] that [his] photo was uploaded
 25 to Shutterfly’s website from a device that was physically located in Illinois and had been
 26 assigned an Illinois-based IP address”); *Rivera*, 238 F. Supp. 3d at 1101 (plaintiff’s

“photographs were allegedly ‘automatically uploaded in Illinois to [Google’s] cloud-based Google Photos service . . . from an Illinois-based Internet Protocol (‘IP’) address’”) (citation omitted). Here, by contrast, Plaintiffs allege that they uploaded their photos from their devices in Illinois directly to *Flickr*; they do not allege that they uploaded *anything* to Amazon (or even IBM). Indeed, Plaintiffs do not allege that they ever interacted with Amazon at all—in Illinois or anywhere else—or that Amazon had any interactions in Illinois concerning the collection, use, or profit from the Dataset in question.

In short, the Complaint does not state a BIPA claim because it does not allege that any facts satisfying the elements of that claim occurred “primarily and substantially” in Illinois, as required to state a claim under Illinois law. *Avery*, 835 N.E.2d at 854; *see also Neals v. PAR Tech. Corp.*, 419 F. Supp. 3d 1088, 1091–92 (N.D. Ill. 2019) (dismissing BIPA complaint with leave to amend where court was “unable to reasonably infer from the complaint that [plaintiff’s] fingerprint was collected in Illinois”); *Tarzian v. Kraft Heinz Foods Co.*, 2019 WL 5064732, at *3 (N.D. Ill. Oct. 9, 2019) (dismissing Illinois consumer fraud claims under Rule 12(b)(6) based on absence of Illinois connection).

B. Plaintiffs’ BIPA Claims Violate the Dormant Commerce Clause.

1. Plaintiffs’ Claims Impermissibly Attempt to Regulate Conduct Occurring Entirely Outside of Illinois’s Borders.

Like Illinois’ extraterritoriality doctrine, the U.S. Constitution ensures a state regulates only conduct it has a substantial interest in controlling. Article I, section 8 gives Congress the exclusive power to regulate commerce “among the several states.” This express grant of power implicitly “limit[s] ... the authority of the States to enact legislation affecting interstate commerce” and “precludes the application of a state statute” that has “the practical effect of ... control[ling] conduct beyond the boundaries of the State ... whether or not the commerce has effects within the State.” *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336 n.1 (1989).

1 “[T]he dormant Commerce Clause . . . has at least two emanations”: (1) when a state
 2 statute “discriminates against interstate commerce, or when its effect is to favor in-state
 3 economic interests over out-of-state interests”; and (2) “the direct regulation emanation”—
 4 i.e., “when a state law directly affects transactions that take place across state lines or entirely
 5 outside of the state’s borders.” *Daniels Sharpsmart, Inc. v. Smith*, 889 F.3d 608, 614–15 (9th
 6 Cir. 2018) (quoting *S.D. Myers, Inc. v. City & County of San Francisco*, 253 F.3d 461, 467
 7 (9th Cir. 2001)). If a state statute directly regulates conduct “entirely outside of the state’s
 8 borders,” the statute is “struck down ... without further inquiry.” *Chinatown Neighborhood*
 9 *Ass’n v. Harris*, 794 F.3d 1136, 1145 (9th Cir. 2015) (citation omitted).

10 Here, the “practical effect” of Plaintiffs’ BIPA claims would be to control conduct
 11 entirely beyond Illinois boundaries, given that Plaintiffs do not allege that Amazon engaged in
 12 **any** relevant conduct in Illinois. Plaintiffs’ claims therefore violate the “direct regulation”
 13 emanation of the dormant Commerce Clause by impermissibly attempting to regulate
 14 Amazon’s conduct occurring entirely outside of Illinois. *See, e.g., Daniels Sharpsmart, Inc.*,
 15 889 F.3d at 614–15 (California Medical Waste Management Act likely violated dormant
 16 Commerce Clause by “attempt[ing] to reach beyond the borders of California and control
 17 transactions that occur wholly outside of the State after ... medical waste ... has been removed
 18 from the State”); *Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1322 (9th Cir. 2015)
 19 (“easily conclud[ing] that” use of California statute to regulate terms of art sales outside
 20 California simply because seller resided in California violated dormant Commerce Clause).

21 *Christies* is instructive. *Christies* involved California’s Resale Royalty Act, which
 22 required a seller of fine art to pay the artist a 5% royalty “if the seller resides in California or
 23 the sale takes place in California.” *Id.* (citation omitted). Various artists sued auction houses
 24 and an online retailer for violating the Royalty Act by failing to pay the required royalties on
 25 fine art sales, alleging that “some sales took place in California and that other sales took place
 26

1 outside California but on behalf of a seller who is a resident of California.” *Id.* The Ninth
2 Circuit affirmed the district court’s Rule 12(b)(6) dismissal of the plaintiffs’ claims:

3 [The] Royalty Act requires the payment of royalties to the artist after a sale of
4 fine art whenever “the seller resides in California *or* the sale takes place in
5 California.” Defendants challenge the first clause because it regulates sales
6 that take place outside California. ***Those sales have no necessary connection***
7 ***with the state other than the residency of the seller.*** For example, if a
8 California resident has a part-time apartment in New York, buys a sculpture in
9 New York from a North Dakota artist to furnish her apartment, and later sells
10 the sculpture to a friend in New York, the Act requires the payment of a
11 royalty to the North Dakota artist – even if the sculpture, the artist, and the
12 buyer never traveled to, or had any connection with, California. ***We easily***
13 ***conclude that the royalty requirement, as applied to out-of-state sales by***
14 ***California residents, violates the dormant Commerce Clause.*** . . .

15 *Id.* at 1323–24 (emphasis added) (internal citations omitted).

16 Plaintiffs’ BIPA claims present analogous circumstances: like the California-based art
17 sellers in *Christies*, Plaintiffs’ Illinois residency does not allow them to use BIPA to regulate
18 the transmission of data between two non-Illinois entities (i.e., IBM and Amazon) simply
19 because some of the data purportedly relates to Illinois residents.

20 The courts that have found dormant Commerce Clause challenges premature at the
21 pleading stage have done so based on very different allegations. In finding Shutterfly’s
22 dormant Commerce Clause argument premature at the pleading stage, for example, the
23 *Monroy* court emphasized that plaintiff’s “suit, as well as his proposed class, is confined to
24 individuals whose biometric data was obtained from photographs ***uploaded to Shutterfly in***
25 ***Illinois.***” 2017 WL 4099846, at *7 (emphasis added). As a result the court held that,
26 “[a]pplying BIPA in this case would not entail any regulation of Shutterfly’s gathering and
storage of biometric data obtained outside of Illinois.” *Id.* By contrast, based on the
allegations in the Complaint, “applying BIPA in this case ***would*** [] entail [] regulation of
[Amazon’s] gathering and storage of biometric data obtained outside of Illinois.” *See id.*
(emphasis added).

1 **2. Plaintiffs' BIPA Claims Impermissibly Displace the Legislation**
 2 **and Policy Decisions Made by States Other than Illinois.**

3 The dormant Commerce Clause also prevents “inconsistent legislation arising from the
 4 projection of one state regulatory regime into the jurisdiction of another State.” *Healy*, 491
 5 U.S. at 326–27 n.1. This has particular application where, as here, extraterritorial application
 6 of Illinois law would **displace** the inconsistent policies of the majority of states, including
 7 Washington, where Amazon is incorporated and has its principal place of business.

8 Washington’s Biometric Privacy Law applies only to the use and collection of
 9 biometric information for “commercial purposes.” RCW 19.375.020(1). Plaintiffs do not
 10 allege that Amazon violated the Washington law. They do not allege that Amazon used their
 11 biometrics for a “[c]ommercial purpose”—i.e., “in furtherance of the sale or disclosure to a
 12 third party of a biometric identifier for the purpose of marketing of goods or services when
 13 such goods or services are unrelated to the initial transaction in which a person first gains
 14 possession of an individual’s biometric identifier.” RCW 19.375.010(4). Moreover,
 15 Washington’s law defines “[b]iometric identifier” as “data generated by automatic
 16 measurements of an individual’s biological characteristics ... used to identify a specific
 17 individual,” but specifically excludes from the definition “a ***physical or digital photograph ...***
 18 ***or data generated therefrom.***” RCW 19.375.010(1) (emphasis added). In other words,
 19 Washington’s law specifically **excludes** from its scope the facial-recognition technology at
 20 issue in the Complaint. *See* Compl. ¶¶ 43–46 (alleging that “biometric identifiers and
 21 information” in IBM’s DiF Dataset were obtained from photos).

22 Washington’s and Illinois’s statutes thus have a very different reach, making them
 23 directly inconsistent. Illinois regulates any businesses that “collect, capture, purchase, receive
 24 through trade, or otherwise obtain a person’s ... biometric identifier or biometric information,”
 25 without regard to the purpose of the collection. 740 ILCS 14/15(b). In contrast, Washington
 26 requires notice and consent only for the process of biometric information “enrollment”—

1 which Plaintiffs do not allege Amazon has done—involving “captur[ing] a biometric
 2 identifier of an individual, convert[ing] it into a reference template that cannot be
 3 reconstructed into the original output image, and stor[ing] it in a database that matches the
 4 biometric identifier to a specific individual.” RCW 19.375.020; RCW 19.375.010(5).
 5 Moreover, Washington law regulates the storage of biometric data only for a narrowly defined
 6 type of “commercial purpose,” i.e., “in furtherance of the sale or disclosure to a third party of
 7 a biometric identifier for the purpose of marketing of goods or services.” RCW
 8 19.375.010(4). As a result, the Washington law does not reach Amazon’s conduct, as
 9 Plaintiffs do not allege any effort by Amazon to sell or disclose biometric identifiers for
 10 marketing purposes. Further, were the Court to interpret BIPA as applying to information
 11 obtained from photos (which it should not, for the reasons explained below), the Illinois law
 12 would again conflict with Washington law, given Washington’s explicit decision *not* to
 13 regulate “data generated” from “a physical or digital photograph.” RCW 19.375.010(1).

14 Allowing Plaintiffs’ BIPA claims to proceed despite these differences between the
 15 Washington Biometric Privacy Law and BIPA would effectively allow Illinois to make policy
 16 and legislative decisions for Washington, when Washington struck a different balance
 17 regarding biometric privacy. Plaintiffs might argue that the laws do not “conflict” because a
 18 company could simultaneously comply with both statutes. But it could only do so by
 19 complying with the stricter statute (BIPA), a result that would effectively “forc[e]
 20 [Washington] to alter [its] regulations to conform with the conflicting legislation.” *Nat’l*
 21 *Solid Wastes Mgmt. Ass’n v. Meyer*, 63 F.3d 652, 660 n.9 (7th Cir. 1995).

22 The dormant Commerce Clause is not violated only where it is logically impossible to
 23 comply with the laws of different states. In *Miller*, for example, Nevada’s statute “require[d]
 24 any national collegiate athletic association to provide a Nevada institution, employee, student-
 25 athlete, or booster who is accused of a rules infraction” with “procedural due process
 26 protections,” many of which were “not included in the NCAA enforcement program.” *Miller*,

1 10 F.3d at 637. The Nevada statute did not literally “conflict” with NCAA rules or the laws
 2 of other states; it was simply stricter in that it required additional protections. The court
 3 nonetheless held that the statute violated the dormant Commerce Clause, and explained what
 4 is meant by states having “inconsistent obligations”:

5 [S]uppose that state X required proof of an infraction beyond a reasonable
 6 doubt, while state Y only required clear and convincing evidence, and state Z
 7 required infractions to be proven by a preponderance of the evidence. Given
 8 that the NCAA must have uniform enforcement procedures in order to
 9 accomplish its fundamental goals, its operation would be disrupted because it
 10 could not possibly comply with all three statutes. ***Nor would it do to say that
 it need only comply with the most stringent burden of persuasion (beyond a
 reasonable doubt), for a state with a less stringent standard might well
 consider its standard a maximum as well as a minimum.*** The serious risk of
 inconsistent obligations wrought by the extraterritorial effect of the Statute
 demonstrates why it constitutes a per se violation of the Commerce Clause.

11 *Id.* at 639–40 (emphasis added).

12 Applied here, BIPA and the Washington Biometric Privacy Law are similarly
 13 inconsistent because the “state with a less stringent” biometric privacy law (Washington)
 14 “might well consider its standard a maximum as well as a minimum.” For instance, perhaps
 15 not wanting to hamper research and development in a state known for technological
 16 innovation, the Washington legislature may have consciously narrowed the scope of its law so
 17 companies do not cease technological development for fear of liability.

18 The dormant Commerce Clause protects businesses engaged in interstate commerce
 19 from precisely this kind of inconsistency between state statutes, which can “easily subject the
 20 [defendant] to conflicting requirements.” *See, e.g., Nat’l Collegiate Athletic Ass’n v. Miller*,
 21 10 F.3d 633, 639 (9th Cir. 1993) (holding Nevada statute establishing “procedural rules for
 22 NCAA enforcement proceedings” violated dormant Commerce Clause because other state
 23 “statutes could easily subject the NCAA to conflicting requirements”). This principle is
 24 particularly important in the Internet context. “[C]ourts have long recognized that certain
 25 types of commerce demand consistent treatment,” and “[t]he Internet represents one of those
 26 areas”: “[r]egulation by any single state can only result in chaos, because at least some states

1 will likely enact laws subjecting Internet users to conflicting obligations.” *Am. Libraries*
 2 *Ass’n v. Pataki*, 969 F. Supp. 160, 181 (S.D.N.Y. 1997); *see also Am. Booksellers Found. v.*
 3 *Dean*, 342 F.3d 96, 104 (2d Cir. 2003) (“the internet will soon be seen as falling within the
 4 class of subjects that are protected from State regulation” under dormant Commerce Clause);
 5 *ACLU v. Johnson*, 194 F.3d 1149, 1162 (10th Cir. 1999). At the very least, the “massive
 6 liability brought on by conflicting applicable law could chill ... the rapidly expanding field of
 7 Internet commerce.” *Archdiocese of St. Louis v. Internet Entm’t Grp., Inc.*, 1999 WL 66022,
 8 at *3 (E.D. Mo. Feb. 12, 1999). At worst, these “inconsistent regulatory schemes could
 9 paralyze the development of the Internet altogether.” *Pataki*, 969 F. Supp. at 181.

10 Applying BIPA to regulate a transaction through which Amazon, a Washington
 11 company, allegedly downloaded data from IBM, a New York-based company, would clearly
 12 burden interstate commerce and violate the dormant Commerce Clause. *See Backpage.com,*
 13 *LLC v. McKenna*, 881 F. Supp. 2d 1262, 1285–86 (W.D. Wash. 2012) (Washington statute
 14 likely violated dormant Commerce Clause because: (1) it would regulate “advertisement[s] ...
 15 occurring entirely outside of the state”; (2) the statute’s proposed “screening process would
 16 constitute a significant and costly change to ... corporations that have little to no connection
 17 with the State of Washington” and a “burden [that] would be exponentially exacerbated if
 18 every state were permitted to legislate its own requirements”; and (3) “the Internet is likely a
 19 unique aspect of commerce that demands national treatment”). Amazon’s download of the
 20 DiF Dataset, which IBM created “for the purpose of improving the ability of facial
 21 recognition systems to fairly and accurately identify all individuals,” Compl. ¶ 42, does not
 22 violate Washington law. To apply BIPA to govern transactions of this nature would adversely
 23 affect businesses and universities across the country, who could be forced to stop any research
 24 into facial recognition using any dataset that might contain a small percentage of images of
 25 Illinois residents. *See, e.g., Ira Kemelmacher-Shlizerman et al., The MegaFace Benchmark: 1*
 26 *Million Faces for Recognition at Scale*, UNIVERSITY OF WASHINGTON (2015),

1 <http://megaface.cs.washington.edu/KemelmacherMegaFaceCVPR16.pdf>, at § 3 (explaining
2 that University of Washington’s “MegaFace” facial-recognition research project made use of
3 “Yahoo’s 100M Flickr set”). The dormant Commerce Clause prevents a single state from
4 imposing this kind of burden on interstate commerce.

5 **C. Plaintiffs Fail to State a Claim Under BIPA Sections 15(b) Or 15(c).**

6 **1. BIPA Does Not Apply to the Use of Photographs.**

7 Plaintiffs fail to state a claim under either BIPA Section 15(b) or 15(c) because, under
8 the statute’s plain language, BIPA does not apply to photographs or identifiers derived from
9 photographs. In enacting BIPA, the Illinois legislature created two categories of covered
10 biometric data: (1) original sources of information about a person (“biometric identifiers”—
11 defined as a “retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry”);
12 and (2) data extracted or derived from those sources (“biometric information”—defined as
13 “information ... based on an individual’s biometric identifier”). 740 ILCS 14/10. The statute
14 specifically *excludes* photographs from the definition of “biometric identifier,” and because
15 “biometric information” includes *only* information based on a “biometric identifier,”
16 “information derived from” photographs necessarily cannot be “biometric information.” *Id.*

17 In short, the Illinois legislature went out of its way to exclude both photographs and
18 information derived from photographs from BIPA’s scope. The alleged “comprehensive set
19 of annotations of intrinsic facial features” IBM allegedly obtained from Plaintiffs’ Flickr
20 photos and sent to Amazon, Compl. ¶¶ 43, 61, are therefore expressly excluded from the
21 statutory definitions of “biometric identifier” and “biometric information.”

22 The legislative history confirms BIPA’s limited purpose. As BIPA moved toward
23 passage, the definitions of “biometric identifier” and “biometric information” were sharply
24 narrowed. The first Senate version of BIPA defined “biometric identifier” broadly:
25 “Examples of biometric identifiers *include, but are not limited to*,] iris or retinal scans,
26 fingerprints, voiceprints, and *records* of hand or facial geometry.” Sen. Bill 2400, § 10 (Feb.

14, 2008) (emphases added) (attached as **Exhibit A**). And although the definition of “biometric identifier” always excluded “photographs,” the original definition of “biometric information” did *not* exclude information derived from photographs. *Id.* The next proposal was even broader: “biometric identifier” included “records or scans of hand geometry, facial geometry, or *facial recognition*.” Sen. Am. to Sen. Bill 2400, § 10 (Apr. 11, 2008) (emphasis added) (attached as **Exhibit B**). But that proposal was rejected, and the House offered a substantially narrower version: it (a) changed the definition of “biometric identifiers” from an open-ended set of “[e]xamples” to a narrow list of enumerated sources; (b) removed the broad term “records” of hand or face geometry; and (c) excluded from the definition of “biometric information” all “information derived from items or procedures excluded under the definition of biometric identifiers.” House Am. to Sen. Bill 2400, § 10 (May 28, 2008) (attached as **Exhibit C**). The legislature enacted this narrower version of BIPA. Consistent with its findings, the legislature expressly declined to include a “record” of facial geometry in the definition of biometric identifier, to regulate all forms of “facial recognition,” or to allow information derived from photographs to slip into the definition of “biometric information.” This reflects a clear intent to regulate only a narrow set of technologies and to exclude a host of others, including all forms of facial recognition derived from photographs.

Although some courts have denied motions to dismiss BIPA complaints based on the application of facial-recognition technology to photos, those non-binding cases were wrongly decided, and this Court should decline to follow them. For example, the court in *In re Facebook Biometric Information Privacy Litigation*, 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016), concluded that “[p]hotographs” is better understood to mean paper prints of photographs, not digitized images stored as a computer file and uploaded to the Internet.” But this reading cannot be reconciled with the commonly understood meaning of “photograph” when the statute was passed in 2008. By 2006, even the Oxford English Dictionary defined “photograph” as “[a] picture made using a camera in which an image is focused on to

1 sensitive material and then made visible and permanent by chemical treatment; (later also) *a*
 2 ***picture made by focusing an image and then storing it digitally.***” Oxford English Dictionary
 3 (Mar. 2006), *available at*
 4 <https://www.oed.com/view/Entry/142818?rskey=8jt7S7&result=1&isAdvanced=false#eid>
 5 (emphasis added); *see also* Webster’s Dictionary 373 (2008 ed.) (“photography” means “the
 6 art or process of producing images on a sensitive surface (as film or a CCD chip [a form of
 7 technology commonly used in digital imaging] by the action of light”), attached as **Exhibit D.**

8 A statutory term should be interpreted “consistent with standard definitions ... found
 9 in dictionaries, which [courts] may consult when attempting to ascertain the plain and
 10 ordinary meaning.” *Rosenbach v. Six Flags Entm’t Corp.*, 129 N.E.3d 1197, 1205 (Ill. 2019).
 11 By interpreting “[p]hotographs” to mean only “paper prints of photographs, not digitized
 12 images,” 185 F. Supp. 3d at 1171, *Facebook* ignored the “plain and ordinary meaning” of
 13 “photographs.” The reasoning in *Monroy* and *Rivera* is similarly unsound, as those cases did
 14 not properly account for BIPA Section 5, which makes clear that the statute is intended to
 15 regulate “biometric identifier-facilitated ***transactions***,” such as those that occur “at grocery
 16 stores, gas stations, and school cafeterias,” which are all intrinsically ***in-person*** activities. 740
 17 ILCS 14/5(b)–(e) (emphases added). Indeed, the statute gives several examples of the
 18 activities it regulates, and ***all*** involve in-person activities in which biometric information
 19 might be captured. *See id.*

20 2. **Plaintiffs Cannot State a Section 15(b) Claim Because they Fail to** 21 **Adequately Allege that Amazon “Collected” or “Otherwise** **Obtained” Their Biometrics.**

22 BIPA Section 15(b) requires private entities, before they can collect an individual’s
 23 biometric information, to: (1) inform the individual “in writing that a biometric identifier or
 24 biometric information is being collected”; (2) inform the individual “in writing of the specific
 25 purpose and length of term for which a biometric identifier or biometric information is being
 26 collected”; and (3) receive “a written release executed by the subject.” 740 ILCS 14/15(b).

1 Unlike BIPA Sections 15(a), (c), (d), and (e)—which use the passive term “in possession”—
 2 only **actions** trigger Section 15(b), i.e., the private entity must “collect, capture, purchase,
 3 receive through trade,” or “obtain” biometric information. 740 ILCS 14/15. Section 15(b)
 4 does not impose any requirements on entities that merely “possess[]” biometric information,
 5 but rather only on entities who actively “collect” biometric information. Had the legislature
 6 meant to bring all entities who merely “possess” biometrics within Section 15(b)’s purview, it
 7 could have explicitly done so, as it did in Sections 15(a), (c), (d), and (e). *See, e.g., Dana*
 8 *Tank Container, Inc. v. Human Rights Comm’n*, 687 N.E.2d 102, 104 (Ill. App. Ct. 1997)
 9 (“Where the legislature uses certain words in one instance and different words in another, it
 10 intended different results.”); *accord, In re D.W.*, 827 N.E.2d 466, 479 (Ill. 2005).

11 Because of this textual difference, Section 15(b) does not apply to the conduct alleged
 12 here, where Plaintiffs do not allege that Amazon collected or obtained biometric data directly
 13 from any individual, let alone these Plaintiffs. *See, e.g., Cameron v. Polar Tech Indus., Inc.*
 14 *& ADP, LLC*, No. 2019-CH-000013, Tr. at 29–36 (DeKalb Cty. Ill. Cir. Ct. Aug. 23, 2019)
 15 (dismissing Section 15(b) claim against third-party timekeeping vendor) (attached as
 16 **Exhibit E**); *Bernal v. ADP, LLC*, No. 2017-CH-12364, Order at 2–3 (Cook Cty. Ill. Cir. Ct.
 17 Aug. 23, 2019) (dismissing Section 15(a), (b), (c), and (d) claims against ADP and noting that
 18 Section 15(b)’s “requirement that the private entity whose actions the subsection is meant to
 19 regulate must receive a ‘written release’ ... does suggest that the legislature did not intend for
 20 the subsection to apply to a third party entity”) (attached as **Exhibit F**); *see also Heard v.*
 21 *Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 966 (N.D. Ill. 2020) (“[F]or Section 15(b)’s
 22 requirements to apply, an entity must, at a minimum, take an active step to ‘collect, capture,
 23 purchase, receive through trade, or otherwise obtain’ biometric data.”) (citation omitted);
 24 *Aisha Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019) (dismissing
 25 Section 15(b) claims against third-party timekeeping vendor and noting that “there is a
 26 difference between *possessing* and *collecting* biometric information”).

1 It would yield absurd results to construe Section 15(b) as imposing individual notice
 2 and release obligations on third parties like Amazon, who do not collect **any** individual's
 3 biometric information but simply download a large dataset of anonymized images that, only
 4 incidentally, **might** include some images of Illinois residents. Plaintiffs' proposed solution
 5 only compounds the problem. They allege that Amazon should have identified Plaintiffs'
 6 images by clicking the one million "links Defendant Amazon received from IBM,"
 7 ascertained that each of Plaintiff's photographs in the DiF Dataset "originated from, and was
 8 affiliated with, his Flickr account," learned of Plaintiff's Illinois residency by scrutinizing the
 9 account, and then contacted each Plaintiff to seek an individual release. Compl. ¶¶ 68–72
 10 (Vance), 76–80 (Janecyk). Leaving aside the absurdity and impracticality of this suggestion,
 11 it would not even satisfy Section 15(b) as Plaintiffs read it, since the statute forbids an entity's
 12 receipt of biometric information unless it "*first*" provides notice and secures a release,
 13 something the Complaint concedes Amazon could not have done until **after** it had the DiF
 14 Dataset in its possession for a sufficient length of time to scour one million Flickr accounts,
 15 locate Plaintiffs, identify them as Illinois residents, and secure a release.

16 In short, under Plaintiffs' reading of the statute, no entity could safely download **any**
 17 large dataset that might contain "biometric information," no matter how anonymized the
 18 images or laudable its purposes, because the of the entity would face BIPA liability if the
 19 dataset happened to contain images of Illinois residents, which the entity could ascertain only
 20 after it was too late to avoid liability. "[T]o read BIPA as requiring that a third party ...,
 21 without any direct relationship with [plaintiffs], obtain written releases from said [plaintiffs]
 22 would be unquestionably not only inconvenient but arguably absurd." *Bernal*, No. 2017-CH-
 23 12364, Ex. F at 2–3. The Court should dismiss Plaintiffs' BIPA Section 15(b) claim because
 24 Plaintiffs do not allege Amazon actively collected or obtained their biometrics.

1 **3. Plaintiffs Cannot Plead a Section 15(c) Claim because they Fail to**
 2 **Plausibly Allege that Amazon “Profited” from Their Biometrics.**

3 Plaintiffs’ BIPA Section 15(c) claim—based on Amazon allegedly “profiting” from
 4 Plaintiffs’ biometrics by using the DiF Database to improve its facial-recognition technology,
 5 *see* Compl. ¶ 65—turns on a mischaracterization of “profit” as used in Section 15(c). That
 6 section provides that an entity may not “sell, lease, trade, or otherwise profit from a person’s
 7 ... biometric identifier or biometric information.” The four verbs—“sell, lease, trade, or
 8 otherwise profit”—all contemplate the direct provision of biometric data in exchange for
 9 money. 740 ILCS 14/15(c). “[W]hen a statutory clause specifically describes several classes
 10 of ... things and then includes ‘other ... things,’ the word ‘other’ is interpreted to mean ‘other
 11 such like.’” *Pooh-Bah Enter., Inc. v. Cnty. of Cook*, 905 N.E.2d 781, 799 (Ill. 2009). Thus,
 12 like “sell,” “lease,” and “trade,” Section 15(c)’s use of “otherwise profit” contemplates an
 13 entity receiving a pecuniary benefit in exchange for a person’s biometric data—not the
 14 indirect “profit” gained by using a large dataset of information derived from anonymous facial
 15 imagery “to improve the fairness and accuracy of ... facial recognition.” Compl. ¶ 62.
 16 Moreover, Plaintiffs have not alleged, and cannot allege, that any of their images in particular
 17 were of any value to Amazon in improving its facial recognition technology, let alone that any
 18 improvements derived from their images led to profits.

19 **II. THE COURT SHOULD DISMISS PLAINTIFFS’ UNJUST ENRICHMENT**
 20 **CLAIM.**

21 Plaintiffs must plead three elements to allege unjust enrichment under Washington
 22 law: “(1) that [Amazon] received a benefit, (2) at [Plaintiffs’] expense, and (3) the
 23 circumstances make it unjust for [Amazon] to retain the benefit without payment.”
 24 *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1129 (W.D. Wash. 2012) (Coughenour,
 25 J.) (citing *Young v. Young*, 191 P.3d 1258, 1262 (Wash. 2008)). Illinois law is no different.
 26 *See Cleary v. Philip Morris Inc.*, 656 F.3d 511, 516 (7th Cir. 2011) (quoting *HPI Health Care*

1 *Servs., Inc. v. Mt. Vernon Hosp., Inc.*, 545 N.E.2d 672, 679, 131 Ill. 2d 145 (Ill. 1989)) (“In
 2 Illinois, ‘[t]o state a cause of action based on a theory of unjust enrichment, a plaintiff must
 3 allege that the defendant has unjustly retained a benefit to the plaintiff’s detriment, and that
 4 defendant’s retention of the benefit violates the fundamental principles of justice, equity, and
 5 good conscience.”). “In the absence of a conflict [between Illinois and Washington law],
 6 Washington law applies,” since it is the law of the forum state. *Kelley v. Microsoft Corp.*, 251
 7 F.R.D. 544, 550 (W.D. Wash. 2008).

8 Plaintiffs’ unjust enrichment claim should be dismissed for at least three reasons:

9 *First*, as explained above, the conduct at issue does not violate any applicable law, and
 10 Plaintiffs have not alleged anything independent of BIPA that would make Amazon’s alleged
 11 conduct “inequitable.” In fact, nothing in the Complaint suggests Plaintiffs’ Flickr photos
 12 were privately posted; to the contrary, Plaintiffs suggest their images were publicly available
 13 to anyone. *See* Compl. ¶¶ 70, 78.

14 *Second*, although Plaintiffs allege the DiF Dataset, consisting of a million images,
 15 indirectly “enriched” Amazon by playing some undefined role in “improv[ing] its facial
 16 recognition products,” *id.* ¶ 65, they do not allege this purported enrichment caused them to
 17 suffer a corresponding economic “expense” or “detriment.” This Court has rejected the
 18 notion that unjust enrichment can be based on alleged misuse of personal or private data,
 19 because unjust enrichment does not apply “outside the context of an ‘expense’ stemming from
 20 some tangible economic loss to a plaintiff.” *Cousineau*, 992 F. Supp. 2d at 1129–30 (granting
 21 motion to dismiss unjust enrichment claim that defendant used location data “to improve its
 22 systems and develop its mobile marketing campaign”); *see also Mount v. PulsePoint, Inc.*,
 23 684 Fed. App’x 32, 36 (2d Cir. 2017), *as amended* (May 3, 2017) (plaintiffs failed to plead
 24 unjust enrichment in light of “plaintiffs’ failure to allege specific loss or deprivation of
 25 opportunity to profit from [personal] information”); *Welborn v. Internal Revenue Serv.*, 218 F.
 26

1 Supp. 3d 64, 78 (D.D.C. 2016) (“Courts have routinely rejected the proposition that an
2 individual’s personal identifying information has an independent monetary value.”).

3 *Third*, unjust enrichment provides an equitable remedy, available only when a plaintiff
4 lacks an adequate remedy at law. As a result, when plaintiffs have a statutory remedy
5 available, “they are not entitled to pursue a remedy in equity” for unjust enrichment. *Seattle*
6 *Profl Eng’g Employees Ass’n v. Boeing Co.*, 139 Wn.2d 824, 838–39, 991 P.2d 1126 (2000)
7 (employees who “had a cause of action under chapter 49.52 RCW” could not pursue equitable
8 claim for restitution or unjust enrichment). Here, Plaintiffs claim that common law principles
9 make it unfair or inequitable for an entity “to improve the fairness and accuracy of its facial
10 recognition products and technologies” by using biometric markers derived from a large
11 dataset of photographs. Compl. ¶ 62. Plaintiffs unjust enrichment claim therefore turns on
12 their allegation of a BIPA violation. In these circumstances, Plaintiffs must pursue their
13 remedies at law, under BIPA, or not at all.

14 **III. PLAINTIFFS HAVE NO SEPARATE INJUNCTIVE RELIEF CLAIM.**

15 Plaintiffs’ purported separate cause of action for injunctive relief fails because
16 “[i]njunctive relief is a remedy, not a cause of action.” *Edifecs Inc., v. TIBCO Software Inc.*,
17 2011 WL 1045645, at *3 (W.D. Wash. Mar. 23, 2011). The Court should also dismiss the
18 request for injunctive relief because Plaintiffs fail to plead viable causes of action in Counts I
19 through III and therefore have no valid claim to which they could tie the requested remedy of
20 injunctive relief. *See, e.g., Edwards v. JPMorgan Chase Bank, N.A.*, 2011 WL 3516155, at
21 *3–4 (W.D. Wash. Aug. 11, 2011) (dismissing injunctive relief claim and noting plaintiffs
22 “have no right to injunctive relief absence a viable cause of action against [defendant]”).

23 **CONCLUSION**

24 For the foregoing reasons, Amazon respectfully requests that the Court dismiss
25 Plaintiffs’ Complaint with prejudice.
26

1 DATED this 14th day of September, 2020.

2
3 DAVIS WRIGHT TREMAINE LLP
Attorneys for Defendant Amazon.com, Inc.

4
5 By /s/ Jaime Drozd Allen
Jaime Drozd Allen, WSBA # 35742
6 David Maas, WSBA # 50694
920 Fifth Avenue, Suite 3300
7 Seattle, WA 98104-1610
Telephone: (206) 757-8039
8 Fax: (206) 757-7039
E-mail: JaimeAllen@dwt.com
9 DavidMaas@dwt.com

10
11 MORGAN LEWIS & BOCKIUS
Attorneys for Defendant Amazon.com, Inc.

12
13 By /s/ Elizabeth B. Herrington
Elizabeth B. Herrington (*pro hac*
14 pending)
77 West Wacker Drive, Suite 500
15 Chicago, IL 60601-5094
Telephone: (312) 324-1188
16 E-mail:
Beth.Herrington@morganlewis.com

17
18 By /s/ Raechel Keay Kummer
Raechel Keay Kummer (*pro hac*
19 pending)
1111 Pennsylvania Avenue, NW
20 Washington, DC 20004-2541
Telephone: (202) 739-3000
21 E-mail:
Raechel.Kummer@morganlewis.com

Exhibit A

SB2400**95TH GENERAL ASSEMBLY****State of Illinois****2007 and 2008****SB2400**

Introduced 2/14/2008, by Sen. Terry Link

SYNOPSIS AS INTRODUCED:

New Act

Creates the Biometric Information Privacy Act. Provides that a public agency or private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the public agency or private entity. Provides that absent a valid warrant or subpoena, a public agency or private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines. Provides that no public agency or private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first satisfies certain conditions. Provides that these provisions do not apply to a public agency engaged in criminal investigations or prosecutions or a public agency acting pursuant to a valid warrant or subpoena. Provides that a public agency in possession of biometric identifiers or biometric information shall store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the public agency stores, transmits, and protects other confidential and sensitive information. Provides that any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court. Preempts home rule. Contains other provisions.

LRB095 19768 KBJ 46142 b

FISCAL NOTE ACT
MAY APPLYHOME RULE NOTE
ACT MAY APPLY**A BILL FOR**

SB2400

LRB095 19768 KBJ 46142 b

1 AN ACT concerning health.

2 **Be it enacted by the People of the State of Illinois,**
3 **represented in the General Assembly:**

4 Section 1. Short title. This Act may be cited as the
5 Biometric Information Privacy Act.

6 Section 5. Legislative findings; intent. The General
7 Assembly finds all of the following:

8 (a) The use of biometrics is growing in the business and
9 security screening sectors and appears to promise streamlined
10 financial transactions and security screenings.

11 (b) Major national corporations have selected the City of
12 Chicago and other locations in this State as pilot testing
13 sites for new applications of biometric-facilitated financial
14 transactions, including "Pay By Touch" at banks, grocery
15 stores, gas stations, and school cafeterias.

16 (c) Biometrics are unlike other unique identifiers that are
17 used to access finances or other sensitive information. For
18 example, social security numbers, when compromised, can be
19 changed. Biometrics, however, are biologically unique to the
20 individual; therefore, once compromised, the individual has no
21 recourse, is at heightened risk for identity theft, and is
22 likely to withdraw from biometric-facilitated transactions.

23 (d) An overwhelming majority of members of the public are

SB2400

- 2 -

LRB095 19768 KBJ 46142 b

1 opposed to the use of biometrics when such information is tied
2 to personal finances and other personal information.

3 (e) Despite limited State law regulating the collection,
4 use, safeguarding, and storage of biometric information, many
5 members of the public are deterred from partaking in biometric
6 identifier-facilitated facility transactions.

7 (f) The public welfare, security, and safety will be served
8 by regulating the collection, use, safeguarding, handling,
9 storage, retention, and destruction of biometric identifiers
10 and information.

11 Section 10. Definitions. In this Act:

12 "Biometric identifier" means any indelible personal
13 physical characteristic which can be used to uniquely identify
14 an individual or pinpoint an individual at a particular place
15 at a particular time. Examples of biometric identifiers
16 include, but are not limited to iris or retinal scans,
17 fingerprints, voiceprints, and records of hand or facial
18 geometry. Biometric identifiers do not include writing
19 samples, written signature, and photographs.

20 "Biometric information" means any information, regardless
21 of how it is captured, converted, stored, or shared, based on
22 an individual's biometric identifier used to identify an
23 individual.

24 "Confidential and sensitive information" means personal
25 information that can be used to uniquely identify an individual

SB2400

- 3 -

LRB095 19768 KBJ 46142 b

1 or an individual's account or property include, but are not
2 limited to a genetic marker, genetic testing information, a
3 unique identifier number to locate an account or property, an
4 account number, a PIN number, a pass code, a driver's license
5 number, or a social security number.

6 "Legally effective written release" means informed written
7 consent.

8 "Private entity" means any individual, partnership,
9 corporation, limited liability company, association, or other
10 group, however organized.

11 "Public agency" means the State of Illinois and its various
12 subdivisions and agencies, and all units of local government,
13 school districts, and other governmental entities.

14 Section 15. Retention; collection; disclosure;
15 destruction.

16 (a) A public agency or private entity in possession of
17 biometric identifiers or biometric information must develop a
18 written policy, made available to the public, establishing a
19 retention schedule and guidelines for permanently destroying
20 biometric identifiers and biometric information when the
21 initial purpose for collecting or obtaining such identifiers or
22 information has been satisfied or within 3 years of the
23 individual's last interaction with the public agency or private
24 entity. Absent a valid warrant or subpoena issued by a court of
25 competent jurisdiction, a public agency or private entity in

SB2400

- 4 -

LRB095 19768 KBJ 46142 b

1 possession of biometric identifiers or biometric information
2 must comply with its established retention schedule and
3 destruction guidelines.

4 (b) No public agency or private entity may collect,
5 capture, purchase, receive through trade, or otherwise obtain a
6 person's or a customer's biometric identifier or biometric
7 information, unless it first:

8 (1) informs the subject in writing that a biometric
9 identifier or biometric information is being collected or
10 stored;

11 (2) informs the subject in writing of the specific
12 purpose and length of term for which a biometric identifier
13 or biometric information is being collected, stored, and
14 used; and

15 (3) receives a legally effective written release
16 executed by the subject of the biometric identifier or
17 biometric information or the subject's legally authorized
18 representative.

19 (c) Subsections (a) and (b) of this Section do not apply to
20 a public agency engaged in criminal investigations or
21 prosecutions. Subsections (a) and (b) of this Section do not
22 apply to a public agency acting pursuant to a valid warrant or
23 subpoena issued by a court of competent jurisdiction.

24 (d) No public agency or private entity in possession of a
25 biometric identifier or biometric information may sell, lease,
26 trade, or otherwise profit from a person's or a customer's

SB2400

- 5 -

LRB095 19768 KBJ 46142 b

1 biometric identifier or biometric information.

2 (e) Nothing in subsection (d) of this Section shall be
3 construed to prohibit or inhibit a public agency engaged in
4 criminal investigations or prosecutions from:

5 (1) sharing biometric identifiers or biometric
6 information with another public agency engaged in criminal
7 investigations or prosecutions to further such criminal
8 investigations or prosecutions;

9 (2) sharing biometric identifiers or biometric
10 information pursuant to federal law or regulation; or

11 (3) sharing biometric identifiers or biometric
12 information pursuant to a valid warrant or subpoena issued
13 by a court of competent jurisdiction.

14 (f) No public agency, private entity, or person in
15 possession of a biometric identifier or biometric information
16 may disclose, redisclose, or otherwise disseminate a person's
17 or a customer's biometric identifier or biometric information,
18 unless:

19 (1) the subject of the biometric identifier or
20 biometric information or the subject's legally authorized
21 representative consents to the disclosure or redisclosure;

22 (2) the disclosure or redisclosure completes a
23 financial transaction requested or authorized by the
24 subject of the biometric identifier or the biometric
25 information;

26 (3) the disclosure or redisclosure is required under

SB2400

- 6 -

LRB095 19768 KBJ 46142 b

1 federal law; and

2 (4) the disclosure is required pursuant to a valid
3 warrant or subpoena issued by a court of competent
4 jurisdiction.

5 (g) A public agency in possession of biometric identifiers
6 or biometric information shall store, transmit, and protect
7 from disclosure all biometric identifiers and biometric
8 information in a manner that is the same as or more protective
9 than the manner in which the public agency stores, transmits,
10 and protects other confidential and sensitive information.

11 (h) A private entity in possession of a biometric
12 identifier or biometric information shall:

13 (1) store, transmit, and protect from disclosure all
14 biometric identifiers and biometric information using the
15 reasonable standard of care within the private entity's
16 industry; and

17 (2) store, transmit, and protect from disclosure all
18 biometric identifiers and biometric information in a
19 manner that is the same as or more protective than the
20 manner in which the private entity stores, transmits, and
21 protects other confidential and sensitive information.

22 (i) All information and records held by a public agency
23 pertaining to biometric identifiers and biometric information
24 shall be confidential and exempt from copying and inspection
25 under the Freedom of Information Act to all except to the
26 subject of the biometric identifier or biometric information.

SB2400

- 7 -

LRB095 19768 KBJ 46142 b

1 The subject of the biometric identifier or biometric
2 information held by a public agency shall be permitted to copy
3 and inspect only their own biometric identifiers and biometric
4 information.

5 Section 20. Right of action.

6 (a) Any person aggrieved by a violation of this Act shall
7 have a right of action in a State circuit court or as a
8 supplemental claim in federal district court against an
9 offending party. A prevailing party may recover for each
10 violation:

11 (1) against any public agency or private entity that
12 negligently violates a provision of this Act, liquidated
13 damages of \$1,000 or actual damages, whichever is greater;

14 (2) against any public agency or private entity that
15 intentionally or recklessly violates a provision of this
16 Act, liquidated damages of \$5,000 or actual damages,
17 whichever is greater;

18 (3) reasonable attorneys' fees and costs, including
19 expert witness fees and other litigation expenses; and

20 (4) other relief, including an injunction, as the State
21 or federal court may deem appropriate.

22 (b) For the purpose of this Act, "prevailing party"
23 includes any party: (i) who obtains some of his or her
24 requested relief through a judicial judgment in his or her
25 favor; (ii) who obtains some of his or her requested relief

SB2400

- 8 -

LRB095 19768 KBJ 46142 b

1 through any settlement agreement approved by the court; or
2 (iii) whose pursuit of a non-frivolous claim was a catalyst for
3 a unilateral change in position by the opposing party relative
4 to the relief sought.

5 Section 25. Home rule. The corporate authorities of a
6 municipality or other unit of local government may enact
7 ordinances, standards, rules, or regulations that protect
8 biometric identifiers and biometric information in a manner or
9 to an extent equal to or greater than the protection provided
10 in this Act. This Section is a limitation on the concurrent
11 exercise of home rule power under subsection (i) of Section 6
12 of Article VII of the Illinois Constitution.

Exhibit B

Sen. Terry Link

Filed: 4/11/2008

09500SB2400sam004

LRB095 19768 RPM 49426 a

1 AMENDMENT TO SENATE BILL 2400

2 AMENDMENT NO. _____. Amend Senate Bill 2400, AS AMENDED,
3 by replacing everything after the enacting clause with the
4 following:

5 "Section 1. Short title. This Act may be cited as the
6 Biometric Information Privacy Act.

7 Section 5. Legislative findings; intent. The General
8 Assembly finds all of the following:

9 (a) The use of biometrics is growing in the business and
10 security screening sectors and appears to promise streamlined
11 financial transactions and security screenings.

12 (b) Major national corporations have selected the City of
13 Chicago and other locations in this State as pilot testing
14 sites for new applications of biometric-facilitated financial
15 transactions, including "Pay By Touch" at banks, grocery
16 stores, gas stations, and school cafeterias.

09500SB2400sam004

-2-

LRB095 19768 RPM 49426 a

1 (c) Biometrics are unlike other unique identifiers that are
2 used to access finances or other sensitive information. For
3 example, social security numbers, when compromised, can be
4 changed. Biometrics, however, are biologically unique to the
5 individual; therefore, once compromised, the individual has no
6 recourse, is at heightened risk for identity theft, and is
7 likely to withdraw from biometric-facilitated transactions.

8 (d) An overwhelming majority of members of the public are
9 opposed to the use of biometrics when such information is tied
10 to personal finances and other personal information.

11 (e) Despite limited State law regulating the collection,
12 use, safeguarding, and storage of biometric information, many
13 members of the public are deterred from partaking in biometric
14 identifier-facilitated facility transactions.

15 (f) The public welfare, security, and safety will be served
16 by regulating the collection, use, safeguarding, handling,
17 storage, retention, and destruction of biometric identifiers
18 and information.

19 Section 10. Definitions. In this Act:

20 "Biometric identifier" means any indelible personal
21 physical characteristic which can be used to uniquely identify
22 an individual or pinpoint an individual at a particular place
23 at a particular time. Examples of biometric identifiers
24 include, but are not limited to iris or retinal scans,
25 fingerprints, voiceprints, and records or scans of hand

09500SB2400sam004

-3-

LRB095 19768 RPM 49426 a

1 geometry, facial geometry, or facial recognition. Biometric
2 identifiers do not include writing samples, written
3 signatures, photographs, tattoo descriptions, physical
4 descriptions, or human biological samples used for valid
5 scientific testing or screening. Biometric identifiers do not
6 include donated organs, tissues, or parts as defined in the
7 Illinois Anatomical Gift Act or blood or serum stored on behalf
8 of recipients or potential recipients of living or cadaveric
9 transplants and obtained or stored by a federally-designated
10 organ procurement agency. Biometric identifiers do not include
11 biological materials regulated under the Genetic Information
12 Privacy Act. Biometric identifiers do not include information
13 captured from a patient in a health care setting or information
14 collected, used, or stored for health care treatment, payment,
15 or operations under the federal Health Insurance Portability
16 and Accountability Act of 1996. Biometric identifiers do not
17 include an X-ray, roentgen process, computed tomography, MRI,
18 PET scan, mammography, or other image or film of the human
19 anatomy used to diagnose, prognose, or treat an illness or
20 other medical condition or to further valid scientific testing
21 or screening.

22 "Biometric information" means any information, regardless
23 of how it is captured, converted, stored, or shared, based on
24 an individual's biometric identifier used to identify an
25 individual. Biometric information does not include information
26 derived from items or procedures excluded under the definition

09500SB2400sam004

-4-

LRB095 19768 RPM 49426 a

1 of biometric identifiers. Biometric information does not
2 include information captured from a patient in a health care
3 setting or information collected, used, or stored for health
4 care treatment, payment, or operations under the federal Health
5 Insurance Portability and Accountability Act of 1996.

6 "Confidential and sensitive information" means personal
7 information that can be used to uniquely identify an individual
8 or an individual's account or property. Examples of
9 confidential and sensitive information include, but are not
10 limited to, a genetic marker, genetic testing information, a
11 unique identifier number to locate an account or property, an
12 account number, a PIN number, a pass code, a driver's license
13 number, or a social security number.

14 "Legally effective written release" means informed written
15 consent or a release executed by an employee as a condition of
16 employment.

17 "Private entity" means any individual, partnership,
18 corporation, limited liability company, association, or other
19 group, however organized. A private entity does not include a
20 public agency. A private entity does not include any court of
21 Illinois, a clerk of the court, or a judge or justice thereof.

22 "Public agency" means the State of Illinois and its various
23 subdivisions and agencies, and all units of local government,
24 school districts, and other governmental entities. A public
25 agency does not include any court of Illinois, a clerk of the
26 court, or a judge or justice thereof.

09500SB2400sam004

-5-

LRB095 19768 RPM 49426 a

1 Section 15. Retention; collection; disclosure;
2 destruction.

3 (a) A public agency or private entity in possession of
4 biometric identifiers or biometric information must develop a
5 written policy, made available to the public, establishing a
6 retention schedule and guidelines for permanently destroying
7 biometric identifiers and biometric information when the
8 initial purpose for collecting or obtaining such identifiers or
9 information has been satisfied or within 3 years of the
10 individual's last interaction with the public agency or private
11 entity, whichever occurs first. Absent a valid warrant or
12 subpoena issued by a court of competent jurisdiction, a public
13 agency or private entity in possession of biometric identifiers
14 or biometric information must comply with its established
15 retention schedule and destruction guidelines.

16 (b) No public agency or private entity may collect,
17 capture, purchase, receive through trade, or otherwise obtain a
18 person's or a customer's biometric identifier or biometric
19 information, unless it first:

20 (1) informs the subject in writing that a biometric
21 identifier or biometric information is being collected or
22 stored;

23 (2) informs the subject in writing of the specific
24 purpose and length of term for which a biometric identifier
25 or biometric information is being collected, stored, and

09500SB2400sam004

-6-

LRB095 19768 RPM 49426 a

1 used; and

2 (3) receives a legally effective written release
3 executed by the subject of the biometric identifier or
4 biometric information or the subject's legally authorized
5 representative.

6 (c) Subsections (a) and (b) of this Section do not apply to
7 a public agency:

8 (1) engaged in criminal investigations, arrests,
9 prosecutions, or law enforcement;

10 (2) overseeing pretrial detention, post-trial
11 commitment, corrections or incarceration, civil
12 commitment, probation services, or parole services;

13 (3) serving as the State central repository of
14 biometrics for criminal identification and investigation
15 purposes;

16 (4) furnishing biometric identifiers or biometric
17 information to a State or federal repository of biometrics
18 pursuant to State or federal law or municipal ordinance;

19 (5) receiving biometric identifiers or biometric
20 information pursuant to State or federal law or municipal
21 ordinance;

22 (6) acting pursuant to a valid warrant or subpoena
23 issued by a court of competent jurisdiction;

24 (7) issuing driver's licenses, driver's permits,
25 identification cards issued pursuant to the Illinois
26 Identification Card Act, or occupational licenses; or

09500SB2400sam004

-7-

LRB095 19768 RPM 49426 a

1 (8) performing employee background checks in
2 accordance with the public agency's hiring policies or
3 statutory obligations.

4 Nothing in subsections (a) and (b) of this Section shall be
5 construed to conflict with the retention and collection
6 practices for fingerprints, other biometric identifiers, or
7 biometric information under the Criminal Identification Act,
8 the Illinois Uniform Conviction Information Act, or the federal
9 National Crime Prevention and Privacy Compact. Subsection (a)
10 of this Section does not apply to school districts; however, a
11 school district that collects biometric identifiers or
12 biometric information must adopt retention schedules and
13 destruction policies in accordance with the School Code.
14 Subsection (a) of this Section does not apply to a fingerprint
15 vendor or fingerprint vendor agency; however, a fingerprint
16 vendor or fingerprint vendor agency must adopt retention
17 schedules and destruction policies in accordance with the
18 Private Detective, Private Alarm, Private Security,
19 Fingerprint Vendor, and Locksmith Act of 2004.

20 (d) No public agency or private entity in possession of a
21 biometric identifier or biometric information may sell, lease,
22 trade, or otherwise profit from a person's or a customer's
23 biometric identifier or biometric information.

24 (e) No public agency or private entity in possession of a
25 biometric identifier or biometric information may disclose,
26 redisclose, or otherwise disseminate a person's or a customer's

09500SB2400sam004

-8-

LRB095 19768 RPM 49426 a

1 biometric identifier or biometric information unless:

2 (1) the subject of the biometric identifier or
3 biometric information or the subject's legally-authorized
4 representative consents to the disclosure or redisclosure;

5 (2) the disclosure or redisclosure completes a
6 financial transaction requested or authorized by the
7 subject of the biometric identifier or the biometric
8 information;

9 (3) the disclosure or redisclosure is required by State
10 or federal law or municipal ordinance; or

11 (4) the disclosure is required pursuant to a valid
12 warrant or subpoena issued by a court of competent
13 jurisdiction.

14 (f) Nothing in subsections (d) or (e) of this Section shall
15 be construed to prohibit or inhibit a public agency (i) engaged
16 in criminal investigations, arrests, prosecutions, or law
17 enforcement, (ii) overseeing pretrial detention, post-trial
18 commitment, corrections or incarceration, civil commitment,
19 probation services, or parole services, (iii) serving as the
20 State central repository of biometrics for criminal
21 identification and investigation purposes, (iv) furnishing
22 biometric identifiers or biometric information to a State or
23 federal repository of biometrics pursuant to State or federal
24 law, or (v) issuing driver's licenses, driver's permits, or
25 identification cards pursuant to the Illinois Identification
26 Card Act from:

09500SB2400sam004

-9-

LRB095 19768 RPM 49426 a

1 (1) sharing biometric identifiers or biometric
2 information with another public agency engaged in criminal
3 investigations, arrests, prosecutions, or law enforcement
4 to further such criminal investigations, arrests,
5 prosecutions, or law enforcement;

6 (2) sharing biometric identifiers or biometric or
7 biometric information with another public agency
8 overseeing pretrial detention, post-trial commitment,
9 corrections or incarceration, civil commitment, probation
10 services, or parole services;

11 (3) sharing biometric identifiers or biometric
12 information pursuant to, or required by, State or federal
13 law; or

14 (4) sharing biometric identifiers or biometric
15 information pursuant to a valid warrant or subpoena issued
16 by a court of competent jurisdiction.

17 (g) Nothing in subsections (d) or (e) of this Section shall
18 be construed to conflict with the reporting and sharing
19 practices for fingerprints, other biometric identifiers, or
20 biometric information under the Criminal Identification Act,
21 the Illinois Uniform Conviction Information Act, and the
22 federal National Crime Prevention and Privacy Compact. Nothing
23 in subsection (d) of this Section shall be construed to
24 conflict with the reporting and sharing practices of a
25 fingerprint vendor or fingerprint vendor agency under the
26 Private Detective, Private Alarm, Private Security,

09500SB2400sam004

-10-

LRB095 19768 RPM 49426 a

1 Fingerprint Vendor, and Locksmith Act of 2004.

2 (h) Nothing in subsections (d) or (e) of this Section shall
3 be construed to prohibit or inhibit a public agency that issues
4 occupational licenses from:

5 (1) sharing biometric identifiers or biometric
6 information pursuant to or when required by State or
7 federal law; or

8 (2) sharing biometric identifiers or biometric
9 information pursuant to a valid warrant or subpoena issued
10 by a court of competent jurisdiction.

11 (i) Nothing in subsections (d) or (e) of this Section shall
12 be construed to prohibit a public agency from performing
13 employee background checks in accordance with the public
14 agency's hiring policies or statutory obligations.

15 (j) A public agency in possession of biometric identifiers
16 or biometric information shall store, transmit, and protect
17 from disclosure all biometric identifiers and biometric
18 information in a reasonable manner that is the same as or more
19 protective than the manner in which the public agency stores,
20 transmits, and protects other similar confidential and
21 sensitive information specific to that public agency. The
22 storage, transmittal, and protection from disclosure standards
23 under this subsection (j) are solely the choice of the public
24 agency to adopt in accordance with this Act, other applicable
25 State or federal law, evolving advances in technology, budget
26 constraints, and comparable practices specific to that public

09500SB2400sam004

-11-

LRB095 19768 RPM 49426 a

1 agency.

2 (k) A private entity in possession of a biometric
3 identifier or biometric information shall:

4 (1) store, transmit, and protect from disclosure all
5 biometric identifiers and biometric information using the
6 reasonable standard of care within the private entity's
7 industry; and

8 (2) store, transmit, and protect from disclosure all
9 biometric identifiers and biometric information in a
10 manner that is the same as or more protective than the
11 manner in which the private entity stores, transmits, and
12 protects other confidential and sensitive information.

13 (l) All information and records held by a public agency
14 pertaining to biometric identifiers and biometric information
15 shall be confidential and exempt from copying and inspection
16 under the Freedom of Information Act to all except to the
17 subject of the biometric identifier or biometric information.
18 The subject of the biometric identifier or biometric
19 information held by a public agency shall be permitted to copy
20 and inspect only their own biometric identifiers and biometric
21 information.

22 Section 20. Right of action. Any person aggrieved by a
23 violation of this Act shall have a right of action in a State
24 circuit court or as a supplemental claim in federal district
25 court against an offending party. A prevailing party may

09500SB2400sam004

-12-

LRB095 19768 RPM 49426 a

1 recover for each violation:

2 (1) against any public agency or private entity that
3 negligently violates a provision of this Act, liquidated
4 damages of \$1,000 or actual damages, whichever is greater;

5 (2) against any public agency or private entity that
6 intentionally or recklessly violates a provision of this
7 Act, liquidated damages of \$5,000 or actual damages,
8 whichever is greater;

9 (3) reasonable attorneys' fees and costs, including
10 expert witness fees and other litigation expenses; and

11 (4) other relief, including an injunction, as the State
12 or federal court may deem appropriate.

13 Section 25. Construction. Nothing in this Act shall be
14 construed to impact the admission or discovery of biometric
15 identifiers and biometric information in any action of any kind
16 in any court, or before any tribunal, board, agency, or person.
17 Nothing in this Act shall be construed to conflict with the
18 X-Ray Retention Act or the federal Health Insurance Portability
19 and Accountability Act of 1996. Subcontractors or agents of a
20 public agency must comply with this Act to the extent and
21 manner this Act applies to that public agency.

22 Section 30. Home rule. Any home rule unit of local
23 government, any non home rule municipality, or any non home
24 rule county within the unincorporated territory of the county

09500SB2400sam004

-13-

LRB095 19768 RPM 49426 a

1 may enact ordinances, standards, rules, or regulations that
2 protect biometric identifiers and biometric information in a
3 manner or to an extent equal to or greater than the protection
4 provided in this Act. This Section is a limitation on the
5 concurrent exercise of home rule power under subsection (i) of
6 Section 6 of Article VII of the Illinois Constitution.

7 Section 95. Applicability. This Act applies to private
8 entities beginning on the effective date of this Act. This Act
9 applies to public agencies beginning on January 1, 2011.

10 Section 99. Effective date. This Act takes effect upon
11 becoming law.".

Exhibit C

Executive Committee

Filed: 5/28/2008

09500SB2400ham001

LRB095 19768 RPM 51505 a

1 AMENDMENT TO SENATE BILL 2400

2 AMENDMENT NO. _____. Amend Senate Bill 2400 by replacing
3 everything after the enacting clause with the following:

4 "Section 1. Short title. This Act may be cited as the
5 Biometric Information Privacy Act.

6 Section 5. Legislative findings; intent. The General
7 Assembly finds all of the following:

8 (a) The use of biometrics is growing in the business and
9 security screening sectors and appears to promise streamlined
10 financial transactions and security screenings.

11 (b) Major national corporations have selected the City of
12 Chicago and other locations in this State as pilot testing
13 sites for new applications of biometric-facilitated financial
14 transactions, including finger-scan technologies at grocery
15 stores, gas stations, and school cafeterias.

16 (c) Biometrics are unlike other unique identifiers that are

09500SB2400ham001

-2-

LRB095 19768 RPM 51505 a

1 used to access finances or other sensitive information. For
2 example, social security numbers, when compromised, can be
3 changed. Biometrics, however, are biologically unique to the
4 individual; therefore, once compromised, the individual has no
5 recourse, is at heightened risk for identity theft, and is
6 likely to withdraw from biometric-facilitated transactions.

7 (d) An overwhelming majority of members of the public are
8 weary of the use of biometrics when such information is tied to
9 finances and other personal information.

10 (e) Despite limited State law regulating the collection,
11 use, safeguarding, and storage of biometrics, many members of
12 the public are deterred from partaking in biometric
13 identifier-facilitated transactions.

14 (f) The full ramifications of biometric technology are not
15 fully known.

16 (g) The public welfare, security, and safety will be served
17 by regulating the collection, use, safeguarding, handling,
18 storage, retention, and destruction of biometric identifiers
19 and information.

20 Section 10. Definitions. In this Act:

21 "Biometric identifier" means a retina or iris scan,
22 fingerprint, voiceprint, or scan of hand or face geometry.
23 Biometric identifiers do not include writing samples, written
24 signatures, photographs, human biological samples used for
25 valid scientific testing or screening, demographic data,

09500SB2400ham001

-3-

LRB095 19768 RPM 51505 a

1 tattoo descriptions, or physical descriptions such as height,
2 weight, hair color, or eye color. Biometric identifiers do not
3 include donated organs, tissues, or parts as defined in the
4 Illinois Anatomical Gift Act or blood or serum stored on behalf
5 of recipients or potential recipients of living or cadaveric
6 transplants and obtained or stored by a federally designated
7 organ procurement agency. Biometric identifiers do not include
8 biological materials regulated under the Genetic Information
9 Privacy Act. Biometric identifiers do not include information
10 captured from a patient in a health care setting or information
11 collected, used, or stored for health care treatment, payment,
12 or operations under the federal Health Insurance Portability
13 and Accountability Act of 1996. Biometric identifiers do not
14 include an X-ray, roentgen process, computed tomography, MRI,
15 PET scan, mammography, or other image or film of the human
16 anatomy used to diagnose, prognose, or treat an illness or
17 other medical condition or to further validate scientific
18 testing or screening.

19 "Biometric information" means any information, regardless
20 of how it is captured, converted, stored, or shared, based on
21 an individual's biometric identifier used to identify an
22 individual. Biometric information does not include information
23 derived from items or procedures excluded under the definition
24 of biometric identifiers.

25 "Confidential and sensitive information" means personal
26 information that can be used to uniquely identify an individual

09500SB2400ham001

-4-

LRB095 19768 RPM 51505 a

1 or an individual's account or property. Examples of
2 confidential and sensitive information include, but are not
3 limited to, a genetic marker, genetic testing information, a
4 unique identifier number to locate an account or property, an
5 account number, a PIN number, a pass code, a driver's license
6 number, or a social security number.

7 "Private entity" means any individual, partnership,
8 corporation, limited liability company, association, or other
9 group, however organized. A private entity does not include a
10 State or local government agency. A private entity does not
11 include any court of Illinois, a clerk of the court, or a judge
12 or justice thereof.

13 "Written release" means informed written consent or, in the
14 context of employment, a release executed by an employee as a
15 condition of employment.

16 Section 15. Retention; collection; disclosure;
17 destruction.

18 (a) A private entity in possession of biometric identifiers
19 or biometric information must develop a written policy, made
20 available to the public, establishing a retention schedule and
21 guidelines for permanently destroying biometric identifiers
22 and biometric information when the initial purpose for
23 collecting or obtaining such identifiers or information has
24 been satisfied or within 3 years of the individual's last
25 interaction with the private entity, whichever occurs first.

09500SB2400ham001

-5-

LRB095 19768 RPM 51505 a

1 Absent a valid warrant or subpoena issued by a court of
2 competent jurisdiction, a private entity in possession of
3 biometric identifiers or biometric information must comply
4 with its established retention schedule and destruction
5 guidelines.

6 (b) No private entity may collect, capture, purchase,
7 receive through trade, or otherwise obtain a person's or a
8 customer's biometric identifier or biometric information,
9 unless it first:

10 (1) informs the subject or the subject's legally
11 authorized representative in writing that a biometric
12 identifier or biometric information is being collected or
13 stored;

14 (2) informs the subject or the subject's legally
15 authorized representative in writing of the specific
16 purpose and length of term for which a biometric identifier
17 or biometric information is being collected, stored, and
18 used; and

19 (3) receives a written release executed by the subject
20 of the biometric identifier or biometric information or the
21 subject's legally authorized representative.

22 (c) No private entity in possession of a biometric
23 identifier or biometric information may sell, lease, trade, or
24 otherwise profit from a person's or a customer's biometric
25 identifier or biometric information.

26 (d) No private entity in possession of a biometric

09500SB2400ham001

-6-

LRB095 19768 RPM 51505 a

1 identifier or biometric information may disclose, redisclose,
2 or otherwise disseminate a person's or a customer's biometric
3 identifier or biometric information unless:

4 (1) the subject of the biometric identifier or
5 biometric information or the subject's legally authorized
6 representative consents to the disclosure or redisclosure;

7 (2) the disclosure or redisclosure completes a
8 financial transaction requested or authorized by the
9 subject of the biometric identifier or the biometric
10 information or the subject's legally authorized
11 representative;

12 (3) the disclosure or redisclosure is required by State
13 or federal law or municipal ordinance; or

14 (4) the disclosure is required pursuant to a valid
15 warrant or subpoena issued by a court of competent
16 jurisdiction.

17 (e) A private entity in possession of a biometric
18 identifier or biometric information shall:

19 (1) store, transmit, and protect from disclosure all
20 biometric identifiers and biometric information using the
21 reasonable standard of care within the private entity's
22 industry; and

23 (2) store, transmit, and protect from disclosure all
24 biometric identifiers and biometric information in a
25 manner that is the same as or more protective than the
26 manner in which the private entity stores, transmits, and

09500SB2400ham001

-7-

LRB095 19768 RPM 51505 a

1 protects other confidential and sensitive information.

2 Section 20. Right of action. Any person aggrieved by a
3 violation of this Act shall have a right of action in a State
4 circuit court or as a supplemental claim in federal district
5 court against an offending party. A prevailing party may
6 recover for each violation:

7 (1) against a private entity that negligently violates
8 a provision of this Act, liquidated damages of \$1,000 or
9 actual damages, whichever is greater;

10 (2) against a private entity that intentionally or
11 recklessly violates a provision of this Act, liquidated
12 damages of \$5,000 or actual damages, whichever is greater;

13 (3) reasonable attorneys' fees and costs, including
14 expert witness fees and other litigation expenses; and

15 (4) other relief, including an injunction, as the State
16 or federal court may deem appropriate.

17 Section 25. Construction.

18 (a) Nothing in this Act shall be construed to impact the
19 admission or discovery of biometric identifiers and biometric
20 information in any action of any kind in any court, or before
21 any tribunal, board, agency, or person.

22 (b) Nothing in this Act shall be construed to conflict with
23 the X-Ray Retention Act, the federal Health Insurance
24 Portability and Accountability Act of 1996 and the rules

09500SB2400ham001

-8-

LRB095 19768 RPM 51505 a

1 promulgated under either Act.

2 (c) Nothing in this Act shall be deemed to apply in any
3 manner to a financial institution or an affiliate of a
4 financial institution that is subject to Title V of the federal
5 Gramm-Leach-Bliley Act of 1999 and the rules promulgated
6 thereunder.

7 (d) Nothing in this Act shall be construed to conflict with
8 the Private Detective, Private Alarm, Private Security,
9 Fingerprint Vendor, and Locksmith Act of 2004 and the rules
10 promulgated thereunder.

11 Section 30. Home rule. Any home rule unit of local
12 government, any non-home rule municipality, or any non-home
13 rule county within the unincorporated territory of the county
14 may enact ordinances, standards, rules, or regulations that
15 protect biometric identifiers and biometric information in a
16 manner or to an extent equal to or greater than the protection
17 provided in this Act. This Section is a limitation on the
18 concurrent exercise of home rule power under subsection (i) of
19 Section 6 of Article VII of the Illinois Constitution.

20 Section 35. Biometric Information Privacy Study Committee.

21 (a) The Department of Human Services, in conjunction with
22 Central Management Services, subject to appropriation or other
23 funds made available for this purpose, shall create the
24 Biometric Information Privacy Study Committee, hereafter

09500SB2400ham001

-9-

LRB095 19768 RPM 51505 a

1 referred to as the Committee. The Department of Human Services,
2 in conjunction with Central Management Services, shall provide
3 staff and administrative support to the Committee. The
4 Committee shall examine (i) current policies, procedures, and
5 practices used by State and local governments to protect an
6 individual against unauthorized disclosure of his or her
7 biometric identifiers and biometric information when State or
8 local government requires the individual to provide his or her
9 biometric identifiers to an officer or agency of the State or
10 local government; (ii) issues related to the collection,
11 destruction, security, and ramifications of biometric
12 identifiers, biometric information, and biometric technology;
13 and (iii) technical and procedural changes necessary in order
14 to implement and enforce reasonable, uniform biometric
15 safeguards by State and local government agencies.

16 (b) The Committee shall hold such public hearings as it
17 deems necessary and present a report of its findings and
18 recommendations to the General Assembly before January 1, 2009.
19 The Committee may begin to conduct business upon appointment of
20 a majority of its members. All appointments shall be completed
21 by 4 months prior to the release of the Committee's final
22 report. The Committee shall meet at least twice and at other
23 times at the call of the chair and may conduct meetings by
24 telecommunication, where possible, in order to minimize travel
25 expenses. The Committee shall consist of 27 members appointed
26 as follows:

09500SB2400ham001

-10-

LRB095 19768 RPM 51505 a

1 (1) 2 members appointed by the President of the Senate;

2 (2) 2 members appointed by the Minority Leader of the
3 Senate;

4 (3) 2 members appointed by the Speaker of the House of
5 Representatives;

6 (4) 2 members appointed by the Minority Leader of the
7 House of Representatives;

8 (5) One member representing the Office of the Governor,
9 appointed by the Governor;

10 (6) One member, who shall serve as the chairperson of
11 the Committee, representing the Office of the Attorney
12 General, appointed by the Attorney General;

13 (7) One member representing the Office of the Secretary
14 of the State, appointed by the Secretary of State;

15 (8) One member from each of the following State
16 agencies appointed by their respective heads: Department
17 of Corrections, Department of Public Health, Department of
18 Human Services, Central Management Services, Illinois
19 Commerce Commission, Illinois State Police; Department of
20 Revenue;

21 (9) One member appointed by the chairperson of the
22 Committee, representing the interests of the City of
23 Chicago;

24 (10) 2 members appointed by the chairperson of the
25 Committee, representing the interests of other
26 municipalities;

09500SB2400ham001

-11-

LRB095 19768 RPM 51505 a

1 (11) 2 members appointed by the chairperson of the
2 Committee, representing the interests of public hospitals;
3 and

4 (12) 4 public members appointed by the chairperson of
5 the Committee, representing the interests of the civil
6 liberties community, the electronic privacy community, and
7 government employees.

8 (c) This Section is repealed January 1, 2009.

9 Section 99. Effective date. This Act takes effect upon
10 becoming law.".

Exhibit D

WEBSTER'S Contemporary School & Office Dictionary

- More than 70,000 definitions •
- Up-to-date and easy-to-use •

Created in Cooperation with the Editors of
MERRIAM-WEBSTER

Webster's Contemporary School & Office Dictionary

Created in Cooperation with the Editors of
MERRIAM-WEBSTER



A Division of Merriam-Webster, Incorporated
Springfield, Massachusetts

Copyright © by Merriam-Webster, Incorporated

Federal Street Press is a trademark of Federal Street Press,
a division of Merriam-Webster, Incorporated.

All rights reserved. No part of this book covered by the copyrights hereon
may be reproduced or copied in any form or by any means — graphic,
electronic, or mechanical, including photocopying, taping,
or information storage and retrieval systems —
without written permission of the publisher.

This 2008 edition published by
Federal Street Press
A Division of Merriam-Webster, Incorporated
P.O. Box 281
Springfield, MA 01102

Federal Street Press books are available for bulk purchase for
sales promotion and premium use.

For details write the manager of special sales,
Federal Street Press, P.O. Box 281, Springfield, MA 01102

ISBN 13 978-1-59695-047-4

ISBN 10 1-59695-047-1

Printed in the United States of America

08 09 10 11 12

5 4 3 2 1

photo-chem-i-cal \fō-tō-'ke-mi-kəl\ *adj*: of, relating to, or resulting from the chemical action of radiant energy
photo-com-pose \kəm-'pōz\ *vb*: to compose reading matter for reproduction by means of characters photographed on film — **photo-com-po-si-tion** \kəm-pə-'zi-shən\ *n*
photo-copy \fō-tə-'kã-pē\ *n*: a photographic reproduction of graphic matter — **photocopy** *vb*
photo-elec-tric \fō-tō-i-'lek-trik\ *adj*: relating to an electrical effect due to the interaction of light with matter — **photo-elec-tri-cal-ly** \-tri-k(ə-)lē\ *adv*
photoelectric cell *n*: a device whose electrical properties are modified by the action of light
photo-en-grave \fō-tō-in-'gräv\ *vb*: to make a photoengraving of
photo-en-grav-ing *n*: a process by which an etched printing plate is made from a photograph or drawing; *also*: a print made from such a plate
photo finish *n*: a race finish so close that a photograph of the finish is used to determine the winner
photo-g \fə-'täg\ *n*: PHOTOGRAPHER
photo-ge-nic \fō-tə-'je-nik\ *adj*: eminently suitable esp. aesthetically for being photographed
photo-graph \fō-tə-'gräf\ *n*: a picture taken by photography — **photograph** *vb* — **photo-gra-pher** \fə-'tã-grä-fər\ *n*
photo-gra-phy \fə-'tã-grä-fē\ *n*: the art or process of producing images on a sensitive surface (as film or a CCD chip) by the action of light — **photo-graph-ic** \fō-tə-'gräf-ik\ *adj* — **photo-graph-i-cal-ly** \-fi-k(ə-)lē\ *adv*
photo-gra-vure \fō-tə-'grä-'vyür\ *n*: a process for making prints from an intaglio plate prepared by photographic methods
photo-il-thog-ra-phy \fō-tō-li-'thã-grä-fē\ *n*: the process of photographically transferring a pattern to a surface for etching (as in making an integrated circuit)
photo-m-e-ter \fō-tä-'mā-tər\ *n*: an instrument for measuring the intensity of light — **photo-met-ric** \fō-tə-'me-trik\ *adj* — **photo-m-e-try** \fō-tä-'mā-trē\ *n*
photo-mi-cro-graph \fō-tə-'mī-kro-'gräf\ *n*: a photograph of a microscope image — **photo-mi-cro-graph-ic** \-mī-'krä-grä-fē\ *n*
photo-n \fō-'tän\ *n*: a quantum of electromagnetic radiation
photo op *n*: a situation or event that lends itself to the taking of pictures which favor the individuals photographed
photo-play \fō-tō-'plã\ *n*: MOTION PICTURE
photo-sen-si-tive \fō-tə-'sen-sə-tiv\ *adj*: sensitive or sensitized to the action of radiant energy
photo-sphere \fō-tə-'sfir\ *n*: the luminous surface of a star — **photo-spher-ic** \fō-tə-'sfir-ik, -'sfer-\ *adj*
photo-syn-the-sis \fō-tō-'sin-thä-sas\ *n*: the process by which chlorophyll-containing plants make carbohydrates from water and from carbon dioxide in the air in the presence of light — **photo-syn-the-size** \-siz\ *vb* — **photo-syn-thet-ic** \-sin-'the-tik\ *adj*
phr *abbr* phrase
phrase \frãz\ *n*: 1: a brief expression 2: a group of two or more grammatically related words that form a sense unit expressing a thought
phrase *vb* **phrased**; **phras-ing**: to express in words
phrase-ol-o-gy \frã-zē-'ã-lä-jē\ *n*, *pl* **-gies**: a manner of phrasing: STYLE
phras-ing *n*: style of expression
phre-net-ic *archaic var of* FRENETIC
phren-ic \fre-'nik\ *adj*: of or relating to the diaphragm (< ~ nerves)
phre-nol-o-gy \fri-'nã-lä-jē\ *n*: the study of the conformation of the skull based on the belief that it indicates mental faculties and character traits
phy-lac-tery \fä-'lak-tä-rē\ *n*, *pl* **-ter-ies** 1: one of two small square leather boxes containing slips inscribed with scripture passages and traditionally worn on the left arm and forehead by Jewish men during morning weekday prayers 2: AMULET
phy-lum \fi-'lòm\ *n*, *pl* **phy-la** \-lã\ [NL, fr. Gk *phylon* tribe, race]: a major category in biological classification esp. of animals that ranks above the class and below the kingdom; *also*: a group (as of people) apparently of common origin

phys *abbr* 1 physical 2 physics
phys-ic \fi-'zik\ *n* 1: the profession of medicine 2: MEDICINE; *esp*: PURGATIVE
physic *vb* **phys-icked**; **phys-ick-ing**: PURGE 2
phys-i-cal \fi-'zi-kəl\ *adj* 1: of or relating to nature or the laws of nature 2: material as opposed to mental or spiritual 3: of, relating to, or produced by the forces and operations of physics 4: of or relating to the body — **phys-i-cal-ly** \-k(ə-)lē\ *adv*
physical *n*: PHYSICAL EXAMINATION
physical education *n*: instruction in the development and care of the body ranging from simple calisthenics to training in hygiene, gymnastics, and the performance and management of athletic games
physical examination *n*: an examination of the bodily functions and condition of an individual
phys-i-cal-ize \fi-'zä-kä-'līz\ *vb* **-ized**; **-iz-ing**: to give physical form or expression to
physical science *n*: any of the sciences (as physics and astronomy) that deal primarily with nonliving materials — **physical scientist** *n*
physical therapy *n*: the treatment of disease by physical and mechanical means (as massage, exercise, water, or heat) — **physical therapist** *n*
phy-si-cian \fä-'zi-shən\ *n*: a doctor of medicine
physician's assistant *n*: a person certified to provide basic medical care usu. under a licensed physician's supervision
phys-i-cist \fi-'zä-sist\ *n*: a scientist who specializes in physics
phys-ics \fi-'ziks\ *n* [L *physica*, pl., natural sciences, fr. Gk *physis*, fr. *physis* growth, nature, fr. *phyein* to bring forth] 1: the science of matter and energy and their interactions 2: the physical properties and composition of something
phys-i-og-no-my \fi-'zē-'äg-nə-mē\ *n*, *pl* **-mies**: facial appearance esp. as a reflection of inner character
phys-i-og-ra-phy \fi-'zē-'ã-grä-fē\ *n*: geography dealing with physical features of the earth — **phys-i-og-graph-ic** \fi-'zē-'ã-grä-fik\ *adj*
phys-i-ol-o-gy \fi-'zē-'ã-lä-jē\ *n* 1: a branch of biology dealing with the functions and functioning of living matter and organisms 2: functional processes in an organism or any of its parts — **phys-i-ol-og-i-cal** \-zē-'ã-'lã-jikəl\ or **phys-i-ol-og-ic** \-jik\ *adj* — **phys-i-ol-og-i-cal-ly** \-ji-k(ə-)lē\ *adv* — **phys-i-ol-o-gist** \-zē-'ã-lä-jist\ *n*
phys-i-ther-a-py \fi-'zē-'ð-'ther-ə-pē\ *n*: PHYSICAL THERAPY — **phys-i-ther-a-pist** \-pist\ *n*
phys-ique \fä-'zēk\ *n*: the build of a person's body: bodily constitution
phy-to-chem-i-cal \fi-'tō-'ke-mi-kəl\ *n*: a chemical compound occurring naturally in plants
phy-to-plank-ton \fi-'tō-'plank-tən\ *n*: plant life of the plankton
pi \pi\ *n*, *pl* **pis** \piz\ 1: the 16th letter of the Greek alphabet — Π or π 2: the symbol π denoting the ratio of the circumference of a circle to its diameter; *also*: the ratio itself equal to approximately 3.1416
PI *abbr* private investigator
pi-a-nis-si-mo \pē-'ã-'ni-sä-'mō\ *adv* or *adj*: very softly — used as a direction in music
pi-a-nist \pē-'ã-nist, 'pē-'ã-\ *n*: a person who plays the piano
pi-a-no \pē-'ã-nō\ *adv* or *adj*: SOFTLY — used as a direction in music
piano \pē-'ã-nō\ *n*, *pl* **pianos** [It, short for *pianoforte*, fr. *gravicembalo col piano e forte*, lit., harpsichord with soft and loud; fr. the fact that its tones could be varied in loudness]: a musical instrument having steel strings sounded by felt-covered hammers operated from a keyboard
pi-ano-forte \pē-'ã-nō-'fôr-tä, -tē; pē-'ã-nä-'fört\ *n*: PIANO
pi-as-tre *also* **pi-as-ter** \pē-'as-tär\ *n* — *see* pound at MONEY table
pi-az-za \pē-'ã-zä, *esp* for 1 -'at-sä\ *n*, *pl* **piazzas** or **pi-az-ze** \-at-(ə-)sã, -'ãt-\ [It, fr. L *platea* broad street] 1: an open square esp. in an Italian town 2: a long hall with an arched roof 3 *dial*: VERANDA, PORCH
pi-broch \pē-'brãk\ *n*: a set of variations for the bagpipe
pic \pik\ *n*, *pl* **pics** or **pix** \'piks\ 1: PHOTOGRAPH 2: MOTION PICTURE

Exhibit E

IN THE CIRCUIT COURT OF THE
TWENTY-THIRD JUDICIAL CIRCUIT
DEKALB COUNTY, CHANCERY DIVISION

BRENT CAMERON, Individually,)	
and on behalf of all others)	
similarly situated,)	
)	
)	
Plaintiffs,)	
)	
vs.)	No. 2019-CH-000013
)	
)	
POLAR TECH INDUSTRIES, INC.,)	
and ADP LLC,)	
)	
)	
Defendants.)	

TRANSCRIPT OF PROCEEDINGS at the
hearing of the above-entitled cause before THE
HONORABLE BRADLEY WALLER, Judge of said Court,
in Room 300 of the Dekalb County Courthouse,
133 West State Street, Sycamore, Illinois, on
August 23, 2019, at the hour of 10:00 a.m.

REPORTED BY: Nohemi Salazar-Pitts, CSR
LICENSE NO.: 084-4648

1 APPEARANCES:

2 STEPHAN ZOURAS, LLP, by
3 MS. HALEY R. JENKINS and
4 MR. RYAN F. STEPHAN
5 100 N Riverside Plaza
6 Suite 2150
Chicago, Illinois 60606
(312) 233-1550
hjenkins@stephanzouras.com
rstephan@stephanzouras.com

7 Appeared on behalf of the
8 Plaintiff and the Putative Class;

9 JENNER & BLOCK, LLP, by
10 MR. DAVID C. LAYDEN
11 353 North Clark Street
12 Chicago, Illinois 60654-3456
312.922.9350
dlayden@jenner.com

13 Appeared on behalf of the
14 Defendant ADP LLC;

15 O'HAGAN MEYER, by
16 MR. THOMAS BOWERS
17 One East Wacker Drive
Suite 3400
Chicago, Illinois 60601
312.422.6100
tbowers@ohaganmeyer.com

18
19 Appeared on behalf of Defendant
20 Polar Tech Industries, Inc.
21
22
23
24

1 THE COURT: All right.

2 THE CLERK: Cameron v Polar Tech.

3 THE COURT: Do you want to stay there?

4 You don't have to.

5 MR. LAYDEN: Whatever you prefer, your
6 Honor.

7 THE COURT: As long as you speak up, I
8 have no problem if you'd like to stay right there.

9 I'd like you to identify yourselves
10 from my left to my right, please.

11 MR. BOWERS: Thomas Bowers on behalf of
12 Polar Tech.

13 MR. LAYDEN: Good morning, your Honor.
14 David Layden on behalf of ADP.

15 MS. JENKINS: Haley Jenkins on behalf of
16 the Plaintiffs.

17 MR. STEPHAN: Good morning, Judge. Ryan
18 Stephan on behalf of Plaintiffs.

19 THE COURT: Did you have something you
20 wanted to tender to me?

21 MR. LAYDEN: No, your Honor. If you
22 prefer that we step up, we're happy to do it.
23 Whatever you'd like us to do.

24 THE COURT: Whatever you guys want to do.

1 If you want to have a seat and argue from there,
2 that's perfectly fine. All right?

3 So what's before the court is motions
4 to dismiss. Polar Tech has brought a motion under
5 2-619.1, which, we all know, is a dual motion
6 including 615 and 619. Essentially, their motion
7 is predicated under (a)(5) statute of limitations
8 issue as well as long as (a)(9), and then ADP has
9 filed a 2-615 motion. There is joint response
10 filed by the Plaintiff. There's respective
11 replies. I have had the opportunity to review
12 everything.

13 Who would like to go first on the
14 Defendants' side?

15 MR. LAYDEN: Your Honor --

16 THE COURT: And you can have a seat, by
17 the way. You don't have to stand. Thank you.

18 MR. LAYDEN: Your Honor, we flipped a
19 coin, and I will go first.

20 THE COURT: All right.

21 MR. LAYDEN: Your Honor, as -- and I will
22 obviously repeat a little bit just to try to
23 summarize the high points. ADP's motion first, of
24 all directed, at the Section 15(b) claim of BIPA,

1 which is the portion of BIPA which requires that
2 an entity collecting biometric information covered
3 by the statute provide written notice and consent
4 and obtain written consent or written release.

5 Your Honor, the basis for our motion
6 is that the way that the plain language of the
7 statute is structured, you read the entire
8 statute, you focus on 15(b), is that 15(b) applies
9 only to the entity, we think, collecting the data.
10 This is not applied to any entity that is in
11 possession of the data.

12 And our position is in this case the
13 Plaintiff has alleged, and it's practically
14 Plaintiff's employer, Polar Tech, which actually
15 collected the data. And obviously the employer
16 had control of the workplace, which required that
17 its employees use the biometric and therefore is
18 the collector.

19 We certainly, of course, as we
20 indicate, don't think it is a valid claim against
21 Polar Tech, but we do believe that if anyone is
22 subject to 15(b), it would be Polar Tech. We
23 think that that is clear from the plain language
24 of statute.

1 It's also important, Judge, to focus
2 on the definition of "written release," which is
3 set forth in BIPA, which provides that a written
4 release in the context of employment is a release
5 executed as a condition of employment.

6 And we think, your Honor, that that
7 further affirms our reading of the statute, which
8 is that when you have an employer using biometric
9 technology in the workplace that is covered by the
10 statute, that it is the employer's job to obtain
11 and to provide written notice to get the consent.

12 Plaintiff's position as set forth in
13 their response is basically that any entity that
14 comes into possession of biometric data at any
15 point in time is subject to 15(b). We don't think
16 that's right, your Honor, because, first of all,
17 it would serve to destroy the careful distinction
18 that the general assembly made in using words like
19 "collect" versus "possess."

20 If that's really what the legislature
21 intended, they would have just simply said "any
22 entity coming into possession of biometric data
23 needs to get notice and get consent." That's not
24 what the legislation said, and we think that's

1 very important to recognize.

2 The Plaintiffs also focused on the
3 word "obtain," or actually it said the words
4 "otherwise obtain" at the end of 15(b), and
5 suggested that that's essentially just akin to
6 coming into possession. We don't agree with them,
7 first of all, in line with what I just said, which
8 is that it would collapse the distinction that the
9 legislature made.

10 And second of all, the word
11 "otherwise obtain" comes at the end of a string of
12 other words, "capture," "collect," which all
13 involve, essentially, an active process of
14 obtaining information from the actual individual
15 who has the biometric data, and therefore we think
16 that it needs to be read consistently with that,
17 meaning an interaction with the person who has the
18 biometric data and the opportunity to give notice
19 and obtain release, if that is required.

20 And for all those reasons, we don't
21 believe that the 15(b) claim can stand. And if
22 you look at the complaint, your Honor, it's pretty
23 clear that the specific allegations in the
24 complaint are that Polar Tech was the entity

1 collecting.

2 Certainly, the Plaintiff has included
3 some general allegations that each Defendant or
4 that Defendants actively collected. But I think
5 if you look at the Plaintiff's theory of the case
6 is that Polar Tech used the clock in the workplace
7 to obtain the employees' biometric information and
8 then it was later, according to Plaintiffs,
9 disclosed to ADP, meaning that ADP was not
10 collecting; ADP was receiving it afterwards.
11 That's the theory that we believe is set forth in
12 the complaint. And we believe that that
13 forecloses the Plaintiff from a pleading, a claim,
14 against ADP under Section 15(b).

15 We also would move to dismiss the
16 Section 15(a) claim, your Honor, and that is the
17 one that requires an entity in possession of
18 biometric information covered by the statute to
19 develop a written retention policy.

20 Your Honor, as we have set forth in
21 our brief, the Plaintiff had argued initially that
22 ADP violated it by not providing the policy to
23 Plaintiff. That's not what the statute requires.
24 The Plaintiff seems to have now backed off a

1 little bit and said we have to have a policy.
2 And, your Honor, first of all, that's not what the
3 statute requires. The statute actually has
4 different language. It says you must develop,
5 which to us means plainly that when you come into
6 possession of biometric information, you then must
7 develop a policy.

8 And I think just to be clear here,
9 your Honor -- and we haven't raised a 619 motion,
10 so this may have to be a summary judgment issue if
11 we don't prevail today on this. But ADP had a
12 biometric policy in effect in October 2017. The
13 Plaintiff started working in early 2018, so there
14 is not going to be a Section 15(a) claim against
15 ADP unless the Plaintiff is going to challenge the
16 efficacy of the policy. I don't understand them
17 doing so, but we may have to get to that.

18 So we think that the 15(a) claim
19 fails to state a claim because they just haven't
20 alleged that ADP violated that section of BIPA.

21 And then, your Honor, finally, that
22 leaves us with the alleged claim under 15(d),
23 which is the section of BIPA that deals with
24 disclosure/disseminations. And here what we

1 really have is a very conclusory obligation.

2 In parts of their Complaint, the
3 Plaintiff alleges that Polar Tech has collected
4 and then disclosed to ADP. But then they say,
5 well, ADP also disclosed to cloud storage
6 providers and other vendors. It's actually not
7 true, but for purposes of their pleading, our
8 position is that they haven't pled that that's the
9 issue.

10 THE COURT: Can I ask you a question?

11 MR. LAYDEN: Certainly, your Honor.

12 THE COURT: My understanding is that you
13 concede in your, I think it's your reply, I could
14 be wrong, that there was a -- it was transmitted
15 to a third-party storage provider.

16 MR. LAYDEN: Your Honor, I don't think we
17 did, and if we did, we misspoke, and so I
18 apologize for that. I can tell you also --

19 THE COURT: I want to be accurate.

20 MR. LAYDEN: Sure. Of course. I can
21 tell you, and I realize that we're stepping a
22 little bit outside pleadings, your Honor; but ADP
23 does not disclose or give data to anyone else.
24 The data -- any data that ADP gets stays at ADP.

1 Plaintiffs, obviously, are entitled
2 to allege that, but I just -- I'm telling you what
3 the facts will ultimately show.

4 THE COURT: Just give me a moment because
5 I do not want to state something that is
6 inaccurate.

7 It must have been with the -- I
8 apologize. It must have been what the Plaintiff
9 had alleged, because I'm looking at your reply and
10 I do not see it in here. As a matter of fact, you
11 can test that.

12 So go ahead.

13 MR. LAYDEN: Very well, your Honor. So
14 basically the -- so putting aside what actually
15 happened, because I appreciate in the 615 motion,
16 you need to deal with the specific facts alleged.
17 We understand that. There is no -- there are no
18 specific facts alleged as to a
19 disclosure/dissemination.

20 And even if -- this is obviously
21 assuming, because it's not true. Even if they
22 could allege that ADP had disseminated it to a
23 cloud storage provider, our view is that is not a
24 disclosure/dissemination because -- for two

1 reasons: A, the dictionary definition of
2 disclosure or disseminating would mean essentially
3 to reveal something. It's to reveal to someone
4 who does not have a right to have it.

5 And the cloud storage provider simply
6 provided, essentially, an administrative service,
7 and it would be a significant expansion of BIPA to
8 say that any time a cloud storage provider is ever
9 provided data that there needs to be, essentially,
10 disclosure consent.

11 And, actually, taking Plaintiff's
12 theory to the actual logical conclusion, I think
13 they would say that 15(b) applies to cloud storage
14 providers. So if anyone ever were to switch
15 storage providers, they would have to somehow get
16 back and go to all the people who they collected
17 data from and get that information including
18 former employees. So I think it becomes one
19 whirlpool very, very quickly.

20 So, your Honor, we're not contending
21 that, you know -- as Plaintiff said that, you
22 know, that ADP could do whatever they want with
23 this data, but they can't give it to -- you know,
24 they can't sell it, they can't provide it to

1 people who -- for purposes other than what it has
2 been collected for.

3 But even assuming -- again, it's not
4 true, but even assuming ADP had used a cloud
5 storage provider, we don't believe that it
6 constitutes a disclosure or dissemination under
7 the statute.

8 As a matter of fact, it is in
9 Section 15(b) of the statute, a provision talks
10 about what happens when you transmit data and how
11 you have to deal with it when you transmit it, and
12 then if you transmit it, you're not allowed to
13 disclose it, which to us is further confirmation
14 that not every transmission of data to someone
15 else constitutes disclosure, because otherwise
16 that section doesn't make any sense.

17 So, your Honor, for those reasons --
18 and I'm obviously happy to answer any further
19 questions you have -- we don't believe that the
20 complaint alleges a sufficient claim under BIPA
21 against ADP, and we would ask that it be dismissed
22 with prejudice.

23 THE COURT: And you're also moving to
24 dismiss the common law negligence count as well,

1 correct?

2 MR. LAYDEN: Your Honor, we are. And
3 obviously Plaintiff's counsel can address this.
4 I don't understand they're proceeding on that, at
5 least in other cases they have dropped that claim
6 post Rosenbach. But we are -- to the extent they
7 are proceeding on that, we are, in fact, proposing
8 it for the reasons that we have said at this time.

9 THE COURT: And you are also saying that
10 the statute of limitations issue which was raised
11 by the co-Defendant is premature at this point
12 because the named Plaintiff, whether you pick the
13 one-, two-, five-year statute of limitation, was
14 filed, even in the worst case, within the one-year
15 statute of limitations; is that correct.

16 MR. LAYDEN: Your Honor, that is ADP's
17 view. I don't want to step on Polar Tech's toes.

18 THE COURT: I'm not -- no. I'm the one
19 bringing it up, so you're not stepping on their
20 toes.

21 MR. LAYDEN: You're right. That is what
22 we believe to be the case. But obviously Polar
23 Tech has a relationship with the Plaintiff, and
24 they are aware, obviously, of the facts relating

1 to his employment status. So we are just not in
2 the position to say that, but based on the briefs,
3 that is what we believe.

4 THE COURT: Okay. Very good.

5 All right. The way I'm going to
6 handle this is that I'm going to allow you to
7 respond to ADP, and then you get the last word on
8 your motion, and then we will move to Polar Tech.

9 You're up.

10 MS. JENKINS: Thank you, your Honor. ADP
11 is essentially claiming that only certain sections
12 of BIPA don't apply to it, but the plain language
13 of the statute makes clear that it applies to all
14 private entities that come into possession or that
15 obtained this data, and to private entities as
16 defined by the statute.

17 THE COURT: Can I ask you this question?
18 What data is ADP actually acquiring?

19 MS. JENKINS: Well, your Honor, ADP is
20 the manufacturer of the clock, the manufacturer of
21 the software, and is additionally supporting the
22 services, and they're obtaining whatever data that
23 clock is taking from the Plaintiff. So when he
24 puts his fingerprint on the clock and it takes

1 that fingerprint data from him, that's the data
2 that they're obtaining.

3 THE COURT: Okay. But -- and I know a
4 little bit about this, I think, but, I mean,
5 there's different ways to obtain data. So you can
6 have the data that I think is contemplated by the
7 statute which is that you have somebody's
8 biometric information in the form of a fingerprint
9 or a retina scan, et cetera, as defined, or you
10 can have data that -- I don't know if you're
11 familiar with the terminology of a hash function
12 where a hash function is essentially, as I have
13 always looked at it as, is it's kind of like
14 gibberish, it's encrypted, it's something that --
15 it's like, you know, your password.

16 So if you type in your password, you
17 know, "I love mom," the hash function recognizes
18 that, but it doesn't recognize it word-for-word.
19 So it seems to me it begs the first question:
20 What data, in your view, is ADP actually acquiring
21 from your client?

22 MS. JENKINS: Well, your Honor, the first
23 part is that they may be acquiring his actual
24 biometric identifier, his actual fingerprint; but

1 the statute also contemplates biometric
2 information, which is any information derived from
3 that fingerprint.

4 So even if -- and I'm going to
5 anticipate ADP would argue that they're collecting
6 some encrypted mathematical template of his -- of
7 the fingerprint scan the Plaintiff puts on the
8 time clock. But that is biometric information,
9 and that is data that they're collecting.

10 THE COURT: So you think the statute is
11 broad enough to encompass and include encrypted or
12 hash functions?

13 MS. JENKINS: I do.

14 THE COURT: Go ahead.

15 MR. STEPHAN: And, Judge, if I can add
16 one thing on that.

17 THE COURT: Yes.

18 MR. STEPHAN: And this is sort of how
19 computers work, right? If you look at any image
20 on your computer, there are numbers behind it.
21 That's how the computers communicate. So they
22 don't -- it's not like a hard copy fingerprint
23 that you would see at a police office. So it's
24 how computers communicate, and we clearly believe

1 that's contemplated by the statute.

2 THE COURT: But, to your point, they
3 communicate by use of digits, they communicate by
4 use of codes. So, you know, you could look at the
5 data collected by virtue of the fingerprint or the
6 retina scan and have absolutely no idea what
7 you're looking at.

8 You believe that's contemplated by
9 the statute?

10 MR. STEPHAN: Well, I don't believe that
11 your first part of that is necessarily accurate.
12 Anything that is encrypted can be unencrypted, and
13 oftentimes numbers represent other things. So we
14 do feel like that is included by the statute and
15 we feel that it is under the definition of
16 biometric information covered by the statute.

17 THE COURT: What section would you direct
18 my attention to, of the statute?

19 MS. JENKINS: In Section 14/10 is the
20 definition of biometric information.

21 THE COURT: So your position is
22 biometric -- the biometric identifier and the
23 biometric information, those two coupled together
24 would include encrypted/unencrypted, hash

1 functions, et cetera?

2 MS. JENKINS: Yes.

3 THE COURT: And your position would be
4 under biometric information means any information
5 regardless of how it's been captured, converted,
6 stored, or shared?

7 MS. JENKINS: Exactly.

8 THE COURT: Go ahead. By the way, do you
9 have the case on that?

10 MS. JENKINS: I'm sorry?

11 THE COURT: Do you have a case or cases
12 on that?

13 MS. JENKINS: Not yet. It's still being
14 litigated.

15 But, your Honor --

16 THE COURT: I don't ask questions I don't
17 know answers to, but ahead.

18 MS. JENKINS: So, your Honor, I think one
19 of the important things to remember is that ADP
20 bases its entire business model on the fact that
21 it's collecting this data, sets out to collect
22 this data because it creates the time clocks that
23 do it and software that goes along with it. It
24 integrates those programs into it's various HR and

1 payroll functions that it provides to various
2 employers, and it profits from all of this.

3 So to call them not a collector of
4 the data, we just think would simply inaccurate.
5 It's actually one of the biggest collectors of
6 this type of data, which means it should be the
7 most knowledgeable in this space, the most
8 experienced. It's one of the most vulnerable if
9 attacked, and it's the most culpable here as well.
10 And yet they did nothing absolutely to comply with
11 BIPA.

12 We are at a Section 2-615 motion to
13 dismiss stage, and if you look simply at the
14 pleadings with respect to Section 15(a), we
15 allege, and ADP hasn't really disputed that they
16 possessed the Plaintiff's biometric data.

17 We alleged that they didn't have a
18 written publically available retention and
19 destruction policy, and if discovery bears out
20 that they might have produced that prior to the
21 Plaintiff's employment, so be it, but we are
22 talking about the allegations in the pleadings
23 right now; and under the pleadings and within the
24 boundaries of the complaint, we have properly

1 alleged a claim with respect to 15(a).

2 With respect to Section 15(b), we
3 have alleged, and they don't really dispute it,
4 that they failed to provide the requisite notice
5 under BIPA and they failed to obtain a written
6 release from our client, all before collecting his
7 biometric data. Instead, they just want to write
8 themselves out of the statute, but as we stated
9 before, Section 15(b) applies uniformly to all
10 private entities that collect, capture, or
11 otherwise obtain this data.

12 THE COURT: How would ADP have any sort
13 of privity or the ability to effectuate the
14 elements under B? In other words, it talks about
15 that has to be obtained before the collection of
16 the data, correct? So how would they be in a
17 position to do that?

18 MS. JENKINS: They could easily implement
19 on their own device, you know, a pop-up screen
20 that comes up when the Plaintiff or another
21 individual first uses the device that says, you
22 know -- it has BIPA-compliant written disclosure
23 and asks for their written consent to do so.

24 They could also require their

1 customers, the employers, to include them on any
2 BIPA-complaint disclosure and a release that they
3 provide to their employees prior to collecting the
4 data.

5 There are a number of ways that they
6 could comply with the statute, but they have
7 chosen not to. They then want the Court to
8 believe that collection rests only with the
9 employer, but this position just simply makes no
10 sense.

11 That would be like saying, when the
12 minister passes around the collection plate at
13 church, only the minister is collecting the money
14 and not the church, and we all know that that's
15 not true; and that's not how data works in our
16 day-to-day lives either. It doesn't stay with the
17 initial collector. No data that you provide to
18 one, you know, company or to one venue generally
19 stays with that. It's disseminated across several
20 platforms and integrated into other platforms, as
21 ADP well knows.

22 And with respect, again, to
23 Section 15(d), we have alleged that they had
24 disclosed or disseminated the Plaintiff's

1 biometric data to third parties. And the biggest
2 contention is that the conclusions -- or their
3 allegations are conclusory, but we can't be
4 expected to know at the pleading stage where
5 everything that they have disclosed has gone and
6 who it's gone to.

7 But we do know from our own
8 investigation and from our experience in this
9 field that the data is shared or at least able to
10 be accessed across a number of different platforms
11 by a number of different parties.

12 Again, if discovery bears out that an
13 allegation turns out not to be fruitful, that's an
14 issue for a different time. Based on the
15 pleadings we have alleged that ADP violated
16 Section 15(d). ADP also claims that Section 15(d)
17 requires some sort of public disclosure of
18 Plaintiff's data, but the plain text of BIPA does
19 not require that. It just requires that it be
20 disseminated or disclosed to a third party.

21 You could disclose something to a
22 third party without making it known to the public
23 at large, which is what we have alleged that they
24 have done here.

1 So, again, your Honor, I think it's
2 important to consider that we're still at the
3 pleading stage, and based on the allegations in
4 the Complaint the Plaintiff has properly alleged
5 the violations of Sections 15(a), (b), and (d) of
6 BIPA with respect to ADP.

7 THE COURT: Anything else?

8 MS. JENKINS: Not unless you have
9 questions.

10 THE COURT: Do you have anything?

11 MR. STEPHAN: No, Judge. Thank you.

12 THE COURT: Okay. You get the last word.

13 It's your motion.

14 MR. LAYDEN: Thank you, Judge.

15 So just to re-respond, and
16 actually -- well, to your questions and also to
17 what Plaintiff's counsel said; first of all, the
18 way the technology works, there is no fingerprint
19 involved. The scanning function essentially
20 measures -- it's much, much less precise than a
21 law enforcement fingerprint, so anything that you
22 may have seen on TV or what we think of as actual
23 fingerprints, it's not involved here.

24 The scanning essentially measures a

1 few points on the fingertip, on a portion of the
2 fingertip. It then creates this mathematical
3 template that your Honor referenced; it's
4 encrypted, it's just a series of hexadecimal
5 numbers. That's all that it is. There's no
6 fingerprint stored, there's no image of the
7 fingerprint stored. It's just a series of
8 numbers. So that's what we're dealing with here.

9 And, your Honor, we certainly
10 disagree, and I think I may have previewed this a
11 little bit in my opening remarks. We don't
12 believe this technology is covered by the statute.
13 We do believe, though, that there probably is
14 going to be summary judgment issues as opposed to
15 a -- or maybe a trial issue as opposed to a motion
16 to dismiss issue.

17 So we're not at all conceding that
18 it's covered, and, your Honor, I think your
19 question goes to one of the key arguments we're to
20 be raising, which is it just simply isn't covered.

21 A couple of other points just to
22 respond to what Plaintiff's counsel said, it's
23 actually not true that ADP manufactures the
24 clocks. ADP doesn't. ADP buys the clocks from a

1 company called Kronos that actually manufactures
2 them. And that's important, your Honor, because
3 it goes to something else that Ms. Jenkins said.

4 Your Honor asked whether -- how could
5 ADP have actually obtain, provide notice and get
6 consent, and that's obviously going to be focused
7 on our briefs. And one of the suggestions that
8 Plaintiff's counsel has alleged is we could just
9 build it in the clock software. Well, that's
10 impossible, your Honor. We don't write the clock
11 software; it's Kronos software.

12 So you're essentially suggesting that
13 something that we buy from someone else, we should
14 somehow be required under BIPA to reprogram, which
15 we can't because we don't actually have the source
16 code to provide this onscreen notice.

17 And then the other suggestion Ms.
18 Jenkins made was that we could just rely upon the
19 customers to provide notice and get consent.
20 Well, actually, the problem with that, your Honor,
21 is that BIPA has these \$1,000, \$5,000 per item
22 penalties, and that's a significant risk to ask a
23 company like ADP to run because certainly we would
24 expect that all of our clients would comply with

1 the law in every instance.

2 But when we have the plaintiffs all
3 over this country who are filing these lawsuits by
4 the dozens and hundreds, and so basically for
5 their end, for their response that they make
6 repeatedly, well, you can't just rely upon someone
7 else to take care -- or just rely upon someone
8 else to just take care of any financial liability.
9 We don't think it's workable, and frankly it's not
10 what the statute says, your Honor. The statute
11 says that -- it talks about a collector, it talks
12 about the companies that may become in possession.

13 And, your Honor, Ms. Jenkins' used an
14 interesting analogy, the minister with the
15 collection plate, which is not one I have heard
16 before, but I actually certainly think it is
17 pretty interesting.

18 THE COURT: Well, we have ushers in my
19 church who pass the plate.

20 MR. LAYDEN: Yeah, I was going to say
21 that, but I thought they were ushers, and the
22 minister is not going to have much to do with the
23 ushers just passing it around.

24 But I think actually the analogy

1 works a little bit better if you think about it
2 this way: The minister, or the church, is Polar
3 Tech; the people passing around the collections
4 plate are the supervisors. They are folks in
5 Polar Tech's facility who are in charge of making
6 sure its employees use these clocks to clock in
7 and out of work so they can be paid wages by Polar
8 Tech in connection with their employment of Polar
9 Tech.

10 I don't think it would be reasonable
11 for the Plaintiff to sue all those supervisors
12 individually and say that they were collecting,
13 and try to subject them to 1,000 liability.
14 Instead, I think that the way BIPA works is that
15 the entity that is actually collecting the data
16 for use in its business, which is the employer, is
17 the entity that is the collector, it's not the
18 supervisor, it's not someone like that.

19 So I think actually that analogy does
20 work if you just switch the entities out a little
21 bit. I think that the ushers are the supervisors.

22 So, your Honor, I think for all those
23 reasons, you know, I think that the Plaintiff's
24 response doesn't really quite meet the arguments

1 that we made in the brief. I think that this is a
2 situation where understandably they're really
3 trying to stretch BIPA way beyond its limits in
4 terms of who is covered by this, and I really
5 think that it just creates a real practical
6 problem.

7 We should not be construing laws in
8 ways that make it impractical or impossible for
9 entities to comply, particularly where you have
10 such a draconian penalty scheme in it. And that's
11 really what they're asking for, and it's really
12 kind of a trap for companies like ADP which are
13 marketed for selling its clocks, providing its
14 services.

15 So for those reasons, we don't think
16 there's any basis to apply 15(b) to ADP, and I
17 don't think -- I think that my remarks on 15(a)
18 and 15(d), I think, can stand; and for those
19 reasons, your Honor, we would ask that you grant
20 our motion to dismiss the claims. Thank you.

21 THE COURT: Thank you. This is a very
22 intriguing area for me. I'm going to deal with
23 the simple thing first or simple count first. I
24 did not see that the Plaintiff gave any sort of a

1 response to the, what I'll term the common law
2 negligence claim, but to make the record clear,
3 there is a statutory provision that I believe
4 predominates, and I'm going to dismiss the common
5 law negligence claim with prejudice under
6 619(a)(9).

7 The -- and that also addresses what
8 Polar Tech raised, but in any event, what's really
9 in play here is the statute, and the statute is
10 the Biometric Information Privacy Act found at
11 740 ILCS 14/1 at (c), and it addresses a number of
12 issues.

13 And what, however, is before me today
14 with respect to ADP is a 2-615 motion. And as we
15 all know, 2-615 is the motion under the Code of
16 Civil Procedure that mandates that I look to the
17 four corners of the pleadings and the four corners
18 of the pleadings only, and that's what I have
19 done.

20 I'm admonished that I'm to construe
21 the complaint in the light most favorable to the
22 nonmoving party. It's what I like to call the "so
23 what" motion. So, what you have alleged does not
24 state a cause of action, in this case under the

1 statute that's before me.

2 So diving into this, the complaint --
3 we're going to start with, since both sides have
4 started with 15(b), I'm going to start there.
5 15(b) of the statute provides that no private
6 entity, and I really have not heard, nor did I see
7 in any of the briefs, if you will, there's no
8 dispute, there's no contest, there's no argument
9 that ADP is anything but a private entity.

10 No private entity may collect,
11 capture, purchase, receive through trade or
12 otherwise obtain a person's or a customer's
13 biometric identifier or biometric information
14 unless it first, so in other words, before, it
15 collects, captures, purchases, receives, or
16 otherwise obtains, it first must inform the
17 subject or the subject's legally authorized
18 representative in writing that a biometric
19 identifier or biometric information is being
20 collected or stored;

21 Two, informs the subject or the
22 subject's legally authorized representative in
23 writing of the specific purpose and length of term
24 for which a biometric identifier or biometric

1 information is being collected, stored, and used,
2 and receives a written release executed by the
3 subject of the biometric identifier or biometric
4 information or the subject's legally authorized
5 representative.

6 There's a definition of written
7 release, and that means informed written consent
8 or, in the context of employment, a release
9 executed by an employee as condition of
10 employment. Although not really addressed in any
11 of the briefs, the issue of what is a -- or what's
12 the definition of a legally authorized
13 representative. That's not set forth in the
14 statute. Does that mean the employer? There are
15 no cases that interpret that.

16 So I have to give effect to the plain
17 language of a statute. I'm mandated by the
18 Appellate and Supreme Court to do that. And the
19 best way is to look at the plain language and not
20 to excise out a particular section, but to read
21 the statute in its totality.

22 So it seems to me that trying to give
23 effect to the statute as a whole where a cause of
24 action would accrue would really be under 15(a),

1 (b), (c), (d), and (e), as to what, if you will, a
2 private entity can do with the data as defined in
3 the statute. So to try to give effect to the
4 whole of the statute, it's this court's view that
5 15(b) only applies to an employer and not a third
6 party.

7 It seems to me that trying to give
8 effect to this, the information is, first and
9 foremost, it is a before, unless it first informs
10 the subject or the subject's legally authorized
11 representative. And if I look at the pleading, it
12 seems to me that the intent of this section is for
13 an employer to be, if you will, responsible for
14 providing that information. And I'm trying to
15 give effect to the definition of written release
16 in the employment context, and that by its plain
17 language states that.

18 So I always hate to be on the cutting
19 edge because that branch can get real thin real
20 quick, but unfortunately I don't see a case that
21 is directly on point interpreting this. The
22 statute is fairly new, as we all know, but my view
23 is that it applies when it is an employment
24 situation, which is the allegation here, that it's

1 the employer's responsibility, not a third party,
2 and I'm going to grant the 2-615 motion with
3 respect to 15(b), with prejudice.

4 15(a) does not require that a private
5 entity provide an individual with anything. It
6 is -- what it states specifically, for the record,
7 is that a private entity in possession of
8 biometric identifiers or biometric information
9 must develop a written policy made available to
10 the public establishing a retention schedule and
11 guidelines for permanently destroying biometric
12 identifiers and biometric information, and it goes
13 on. I don't think I need to go any further.

14 But with respect to the pleadings, I
15 think there needs to be more specificity than just
16 a recitation of the statute. But I don't think
17 the pleadings correctly or accurately state that,
18 and I'm directing everyone's attention to
19 paragraph 44, "Furthermore, each defendant fails
20 to provide employees," that's not required, but I
21 am certainly going to give, with respect to a
22 15(a) allegation, the Plaintiff the opportunity to
23 replead. So the 615 motion will be granted,
24 however, it will be granted without prejudice.

1 15(d), this is interesting. 15(d)
2 provides that "no private entity in possession of
3 a biometric identifier or biometric information
4 may disclose, re-disclose or otherwise disseminate
5 a person's or a customer's biometric identifier or
6 biometric information, unless the subject of the
7 biometric identifier or biometric information or
8 the subject's legally authorized representative --
9 there is it is again" -- "consents to the
10 disclosure or re-disclosure, the disclosure or
11 re-disclosure completes a financial transaction
12 requested or authorized by the subject, the
13 biometric identifier, or the biometric
14 information, or the subject's legally authorized
15 representative --" it's not applicable here --
16 "the disclosure or re-disclosure is required by
17 State or Federal Law or municipal ordinance, or
18 the disclosure is required pursuant to a valid
19 warrant or subpoena issued by a court of competent
20 jurisdiction."

21 But what's in play here is no private
22 entity in possession of a biometric identifier or
23 biometric information may disclose re-disclose or
24 otherwise disseminate. With respect to again, the

1 four corners of the pleadings, it seems to me that
2 there are not sufficient facts, there's not
3 sufficient specificity just to say it was
4 disclosed without more.

5 And, again, like I did under (a), I'm
6 going to grant the motion; however, it's going to
7 be without prejudice to replead. And so that will
8 be the order of the Court with respect to ADP's
9 motion.

10 You're up.

11 MR. BOWERS: Thank you, your Honor. And
12 I apologize, I'm also getting over a cold, so I'll
13 do my best to speak up.

14 THE COURT: No apologies necessary.

15 Go ahead.

16 MR. BOWERS: So given the fact that your
17 Honor has already addressed Polar Tech's argument
18 with respect to Plaintiff's Common Law negligence
19 claim, I'll just start turn my attention to the
20 statute of limitations issue that's before you.

21 We filed a Section 619 motion with
22 respect to the statute of limitations --

23 THE COURT: (a)(5)?

24 MR. BOWERS: Correct, (a)(5)motion.

1 As your Honor is well aware, BIPA
2 does not contain an expressed statute of
3 limitations. This is an area that's being
4 litigated amongst circuit courts across Illinois,
5 and these lawsuits continue to be filed by
6 plaintiffs' attorneys in Northern Illinois and
7 across the state.

8 It is Polar Tech's stance that a
9 one-year statute of limitations applies to
10 Mr. Cameron's BIPA claim because BIPA is a statute
11 that is concerned with the right of privacy and
12 the protection of privacy rights.

13 Alternatively, Polar Tech submits
14 that in the event a one-year statute of
15 limitations does not apply, a two-year statute of
16 limitations applies to limit any claims of the
17 Plaintiffs and/or the putative class to two years
18 arising two years before the date of filing the
19 complaint, which in this case would be August 7th
20 of 2016.

21 Based on the fact that the Illinois
22 Supreme Court's decision in *Rosenbach v Six Flags*
23 effectively transformed BIPA into not only a
24 strict liability statute, but also a penal

1 statute, as opposed to a remedial statute, as
2 Plaintiff asserts in his response brief.

3 With respect to Polar Tech's
4 assertion that a one-year statute of limitation
5 applies -- this falls under Section 13-201 of the
6 Code of Civil Procedure, a one-year statute of
7 limitation applies in the event that there is a
8 publication --

9 THE REPORTER: Your Honor, I need him to
10 speak up.

11 THE COURT: Can you speak up a little bit
12 for the court reporter.

13 MR. BOWERS: Yes. Sorry.

14 A one-year statute of limitation
15 applies to privacy claims in the event that there
16 is publication of the information that was, in
17 this case, purportedly collected, stored and, as
18 alleged in Plaintiff's, disseminated.

19 In Plaintiff's Complaint, there are
20 allegations that biometric data was not only
21 collected and stored, but also disseminated to
22 third parties, ADP, and, quote, "other unknown
23 third parties."

24 There is a case out of the First

1 District Appellate Court called Popko v
2 Continental Casualty Company. That cite is 355
3 Ill. App. 3d 257. It's a 2005 case out of the
4 First District. In that case, an employee was
5 terminated from CNA Insurance, Continental
6 Casualty Insurance.

7 After undergoing a performance review
8 in which he allegedly used profanity during this
9 performance review with his supervisor. That
10 supervisor sent a memorandum to yet another
11 supervisor, a manager within the company, and the
12 plaintiff was ultimately terminated in that case.

13 And in that case he brought a
14 defamation claim against his former employer, but
15 the focus of the court's opinion there was whether
16 or not there was publication. And I bring this
17 particular case up, not for the defamation part of
18 the case, but to address the issue of publication.

19 In that case, the court said that
20 there was publication solely by virtue of the fact
21 that information regarding the plaintiff's
22 performance review was transmitted by his
23 supervisor who was present at that performance
24 review to another individual within the company.

1 So in that case, an intra-office communication
2 from one individual to another, while not made
3 directly available to the public at large, can
4 constitute a publication.

5 And similarly here, that's what's
6 been alleged in Plaintiff's Complaint. Plaintiff
7 has alleged that Polar Tech collected and stored
8 Mr. Cameron's biometric data by virtue of his
9 usage of providing scans of his finger on a time
10 clock system that was provided by ADP, and that
11 that information was then disseminated to a third
12 party, in this case ADP, and potentially to other
13 third parties.

14 BIPA itself is concerned with
15 publication, as seen in Section 15(c) and section
16 15(d).

17 THE COURT: Can I stop and ask you a
18 question?

19 MR. BOWERS: Sure.

20 THE COURT: So the allegations in the
21 Complaint is that the Plaintiff was employed by
22 your client from February of 2018 until May of
23 2018, and this is a 619, so you admit all well
24 pled facts. And this case was filed on 8/7 of

1 '18. So would I be correct in assuming that what
2 you're directing my attention to would be the
3 class action component of this pleading?

4 MR. BOWERS: That's correct.

5 THE COURT: Go ahead.

6 MR. BOWERS: So, yes, we are directing
7 your attention to the class action component for
8 this particular claim as opposed to Mr. Cameron's
9 actual dates of employment. But as stated before,
10 BIPA does concern itself with publication in
11 Sections 15(c) and 15(d).

12 THE COURT: But you would agree that, I
13 mean, the Complaint was filed even in the shortest
14 statute of limitation, which is a year that you're
15 asking me to consider, right?

16 MR. BOWERS: Correct.

17 THE COURT: Okay. Go ahead.

18 MR. BOWERS: I will concede the fact that
19 this complaint was filed within one year of
20 Mr. Cameron's employment.

21 THE COURT: Okay.

22 MR. BOWERS: But for purposes of the
23 class size, that will be determined down the road.
24 That's why I preface it now, because I don't want

1 to waive this argument later.

2 THE COURT: I understand.

3 MR. BOWERS: BIPA does prohibit parties
4 from selling and trading or profiting by
5 dissemination of a person's biometric data and
6 also prohibits parties from disclosing
7 re-disclosing, or otherwise disseminating an
8 individual's biometric data, and this signals the
9 Illinois General Assembly's intent to regulate
10 dissemination and, therefore, publication of an
11 individual's biometric data to third parties.

12 Again, publication is not required,
13 that this data be made available to the public at
14 large, or that could be made available to the
15 public at large, it requires that it's transmitted
16 to a third party. Because Illinois takes a more
17 narrow view of what "publication" means as opposed
18 to other jurisdictions in this country.

19 So, accordingly, we submit that a
20 one-year statute of limitations applies to
21 Mr. Cameron's claim.

22 Alternatively, if the Court is
23 inclined that to opine that the one-year statute
24 of limitations does not apply, Polar Tech submits

1 that a two-year statute of limitations applies,
2 because Mr. Cameron seeks a statutory penalty in
3 its prayer for relief.

4 BIPA provides liquidated damages of
5 \$1,000 per negligent violation, and \$5,000 for
6 intention and/or reckless violation of the Act.

7 Plaintiff asserts that a five-year
8 statute of limitations applies to his claim
9 because BIPA does not contain an expressed statute
10 of limitations. And while BIPA itself does not
11 contain a specific statute of limitations, unless
12 a rule to the contrary applies, then the five-year
13 statute of limitations, the catch-all provision,
14 applies. And that's exactly what that is, a
15 catch-all, a backup, if nothing else applies.

16 Here alternatively, a two-year
17 statute of limitations would apply should the
18 one-year statute of limitations not apply, because
19 the Supreme Court's decision in *Rosenbach v Six*
20 *Flags* not only transforms BIPA into a strict
21 liability statute, it also rendered it into a
22 penal statute.

23 A statute is there for penal if it
24 imposes automatic liability or violation of its

1 own terms, if it sets forth a predetermined amount
2 of damages, and if it imposes liability without
3 actual damages suffered by the plaintiff.

4 In Rosenbach, the Supreme Court held
5 that the plaintiff did not need to allege actual
6 damages in order to bring a claim underneath the
7 umbrella of the statute. That is exactly what
8 happened here.

9 Plaintiff then attempts to rebut my
10 argument by saying that BIPA addresses a societal
11 concern, in this case regulating an individual's
12 privacy and their biometric data, which, fine, I
13 will concede that it may have been an intent. But
14 a statute can both be penal and serve remedial
15 purposes.

16 In Plaintiff's response, they bring
17 up the Telephone Consumer Protection Act, and
18 whether -- in the case called Lay, whether or not
19 that statute was remedial or penal. And in that
20 case, the court noted that the TCPA were provided
21 for treble damages, which were separate from the
22 liquidated damages contained within the statute.
23 That's a distinguishing feature from BIPA.

24 BIPA does not contain such a

1 provision. It provides solely liquidated damages.
2 It provides punitive and deterrent goals to
3 prevent abuse of individual -- collection of an
4 individual's biometric data. It is
5 distinguishable from TCPA.

6 And in the event that a one-year
7 statute of limitations does not apply, because the
8 statute is penal in nature, it has deterrent and
9 punitive goals, it provides a predetermined amount
10 of damages, it imposes liability without regard
11 for actual damages as articulated by the Illinois
12 Supreme Court in Rosenbach, and it imposes
13 automatic liability for a violation of its own
14 terms, which the Illinois Supreme Court rendered
15 the statute into a strict liability statute
16 through Rosenbach.

17 This statute is penal in nature, not
18 remedial, and alternatively, a two-year statute of
19 limitations would apply to this lawsuit in
20 general, to BIPA claims in general.

21 THE COURT: Anything else?

22 MR. BOWERS: That's all I have.

23 THE COURT: You will get the last word.

24 MS. JENKINS: Thank you, your Honor.

1 We would first like to acknowledge we
2 do agree with the court. This isn't properly at
3 issue right now. The Plaintiff's claims were
4 filed within one year, so even assuming the short
5 statute of limitations, this complaint cannot be
6 dismissed on those grounds alone.

7 Instead, this is Defendant's improper
8 attempt to limit the class size, which it's more
9 properly handled by the motion for class
10 certification or potentially a summary judgment.
11 But regardless, as it's been noted, BIPA has no
12 self-contained statute of limitations, and
13 therefore, the statute of limitations provided by
14 735 ILCS 5/13-205, which is the default five-year
15 limitations period, should apply.

16

17

18 The one-year statute of limitations
19 does not apply here for two reasons. First, while
20 we might allege that Plaintiff's privacy has been
21 denigrated by virtue of Polar Tech violations of
22 BIPA, the true nature of a potential liability
23 here stems from Polar Tech's violation of the
24 statute itself. This is not an action for slander

1 or libel or publication of a matter violating the
2 right to privacy.

3 The plain and unambiguous language of
4 Section 13-201, which provides the one-year
5 statute of limitations states that it applies to
6 actions for publication of a matter violating the
7 right to privacy, which is not what's being
8 alleged here. The defendants in these cases can't
9 have it both ways saying that publication is a
10 necessary element for the statute of limitations,
11 but dissemination only takes place if it's made to
12 the public at large.

13 The positions that have been taken,
14 and I understand that ADP and Polar Tech were
15 making separate arguments, but these types of
16 positions are inconsistent. And further, the
17 plain and unambiguous language of BIPA doesn't
18 require us to allege publication, and therefore we
19 don't believe that BIPA falls within the one-year
20 statute of limitations period.

21 Polar Tech, alternatively declares
22 that the two-year statute applies because it
23 thinks that BIPA is a penal statute; but penal
24 statutes impose automatic liability, which BIPA

1 does not. It sets forth a predetermined amount of
2 damages, and BIPA does contain statutory damages
3 in the event that Plaintiff doesn't recover their
4 actual damages.

5 They also claim that BIPA imposes
6 damages without regard to the actual damages
7 suffered by the Plaintiff, but that's simply not
8 true. If you read the statute, Section 14/20
9 provides that a plaintiff can recover actual
10 damages or statutory damages, whichever is
11 greater, and, therefore, BIPA is not a penal
12 statute.

13 It is analogous to the Telephone
14 Consumer Protection Act, or TCPA, which provides
15 that a plaintiff can recover actual damages or
16 \$500 per each violation, whichever is greater.
17 The language is almost the same as the language in
18 BIPA.

19 And as the Illinois Supreme Court
20 recognized in Standard Mutual Insurance Company v
21 Lay, the TCPA is not a penal statute with that
22 identical statutory language, and therefore BIPA
23 shouldn't be considered one either.

24 Rosenbach didn't make BIPA a penal

1 statute. It again reiterates that a plaintiff
2 could recover actual damages if they properly pled
3 and proved them or statutory damages. And they
4 don't need to allege actual damages because the
5 statute provides statutory damages. Therefore,
6 only the five-year statute of limitations remains.

7 And furthermore, Judge, no case or
8 court or judge has considered this issue, directly
9 or indirectly has adopted the Defendant's
10 position. Every court that has considered this
11 issue has ruled in favor of the five-year statute
12 of limitations. And I recognize that none of
13 those cases are binding on this court, but we do
14 think that they're persuasive in holding that
15 several judges across both the country and the
16 state have held that the five-year statute of
17 limitations applies.

18 And we filed with the court a notice
19 of supplemental authority. The case Robertson v
20 Hostmark Hospitality Group, which I have copy of
21 if you need it today; and in that case Judge Cohen
22 in Cook County also held that the one-year and
23 two-year statute of limitations do not apply for
24 the reasons we have articulated, and agreed that

1 the five-year statute of limitations period is not
2 applicable here.

3 Other cases, in ruling on motions for
4 class certification, have held that the five-year
5 statute of statute of limitations period is
6 applicable with respect to the class size, and
7 those cases are Alvarado v International Laser
8 Production Inc., Case No. 18-cv-07756 in the
9 Northern District of Illinois decided on June 19
10 of 2019; Roberson v Symphony Post Acute Network,
11 Case No. 17-L-733 in the Circuit Court of St.
12 Clair County, in March of 2019; and the Facebook
13 Biometric Privacy Litigation case pending in the
14 Northern District of California, which was
15 determined and decided in April of 2018.

16 And for these reasons, we believe
17 that the five-year statute of limitations period
18 is the one that applies to BIPA and not this
19 shorter one or two-year periods.

20 THE COURT: Thank you.

21 Last word.

22 MR. BOWERS: Your Honor, just a couple of
23 things to address, and I'll do my best to make
24 this quick.

1 First, Ms. Jenkins has stated earlier
2 that the allegations contained in this complaint
3 focused on the violation of the statute based on
4 the collection of biometric data. They have also
5 alleged that this data was disseminated to third
6 parties, and BIPA itself expressly prohibits
7 dissemination and publication of data to third
8 parties.

9 That is part of the violation of
10 BIPA. There are multiple ways to violate the
11 statute: By profiting, by collecting, by
12 capturing, by storing, by disseminating, by
13 publishing.

14 Publishing and collecting were both
15 alleged in this complaint. BIPA expressly
16 prohibits publishing and disseminating biometric
17 data to third party. That was what was alleged in
18 this complaint. So, accordingly, we would submit
19 that a one-year statute of limitations does apply
20 to this claim.

21 Secondly, with respect to the
22 argument of the two-year statute of limitations,
23 as I have stated before, this statute does contain
24 express liquidated damages based on the type of

1 violation of the statute. It imposes liability
2 automatically for violation of its terms based
3 upon a plain reading and interpretation of the
4 Illinois Supreme Court's decision in Rosenbach.

5 This statute has been transformed
6 into a strict liability statute, and it has been
7 transformed into a penal statute, and
8 alternatively, a two-year statute of limitations
9 should apply to a BIPA claim.

10 And, finally, I'll just bring up the
11 authority, the supplemental authority that
12 Ms. Jenkins has just brought to your attention.
13 None of these cases are -- none of these decisions
14 are binding on this court. We have a decision out
15 of the Northern District of Illinois, at a
16 St. Clair County, and out of the Northern District
17 of California. None of those cases, none of those
18 decisions are a binding precedent on this court.

19 And so accordingly, Polar Tech
20 submits that those decisions should be disregarded
21 as they are not binding on this court.

22 THE COURT: Thank you.

23 Excellent job. But as I thought
24 through this, it seems to me that this is

1 premature. I don't have before me anything more
2 than the complaint which pertains to the named
3 Plaintiff. I understand why you did what you did.
4 You want to preserve this. It is preserved. But
5 I'm going to enter and continue my decision on
6 that until, I don't know, class certification,
7 summary judgment.

8 But certainly, in my view, the record
9 needs to be developed much more than it is, but
10 Polar Tech is in no way, shape, or form
11 prejudiced, precluded, foreclosed from addressing
12 this as we get further down the road. So I am not
13 ruling on this. I'll enter and continue the issue
14 for a later date.

15 That being said, how much time does
16 Plaintiff need to replead on the Counts or the
17 sections that I left up?

18 MS. JENKINS: 30 days, your Honor, if
19 that's okay with you.

20 THE COURT: That's reasonable. Here's
21 the offer that I will make. Okay? I know this is
22 isn't the only file on your respective desks. I
23 don't believe in bringing back attorneys unless
24 we're going to accomplish something of substance,

1 so I will throw this out.

2 I don't know what your respective
3 thoughts are, obviously, because you haven't seen
4 the amended pleading, but I'm affording you ample
5 opportunity to decide whether you're going to file
6 a motion to dismiss; I'm willing to do that.

7 You're all excellent lawyers. You
8 can work out a briefing schedule. I can give you
9 an outside date right now for a hearing date. If
10 it ends up being that you file an answer, we could
11 just use that as a status date on discovery, et
12 cetera.

13 Would you like to take me up on my
14 offer.

15 MR. LAYDEN: It's certainly fine with
16 ADP, your Honor.

17 THE COURT: Why don't we kick this out
18 for status/argument. How about if we go to the
19 beginning of December? That gives each side a
20 full opportunity to work out a briefing schedule,
21 with the caveat that I get courtesy copies one
22 week before, but I'll just throw out arbitrarily
23 Wednesday, December 4th at 10:00 for argument or
24 status.

1 MR. LAYDEN: Your Honor, that day is not
2 terrific for me. Any other day that week is fine.

3 THE COURT: December the 6th? That's a
4 Friday at 10:00.

5 MR. STEPHAN: Judge, can we suggest maybe
6 pushing that to January. The holidays are just --
7 I'm always jammed.

8 THE COURT: I'm not opposed at all.
9 Might I suggest the 17th, 10:00?

10 MR. LAYDEN: Fine with me.

11 THE COURT: Argument or status?

12 MR. BOWERS: Judge, I'm scheduled to be
13 out of town that day. Is there a day that week,
14 maybe earlier that week?

15 THE COURT: 15th?

16 MR. BOWERS: That's fine, your Honor.

17 MR. LAYDEN: That works.

18 MR. STEPHAN: That's good.

19 THE COURT: Same thing. 10:00 status or
20 argument. And then you guys work out a briefing
21 schedule. If somebody wants to e-mail an order,
22 if it gets to that point, I'd be happy to enter
23 the order without a court appearance. Okay?

24 So if you'd indicate today for the

1 reasons stated on the record, and then just go
2 from there.

3 Anything else we can accomplish?

4 MS. JENKINS: No, your Honor.

5 MR. STEPHAN: Thank you, Judge.

6 MR. LAYDEN: Thanks, your Honor.

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

1 STATE OF ILLINOIS)

2)

3 COUNTY OF C O O K)

4

5 NOHEMI SALAZAR-PITTS, a Certified

6 Shorthand Reporter doing business in and for the

7 State of Illinois certifies that she reported in

8 shorthand the proceedings of said hearing, and

9 that the foregoing is a true and correct

10 transcript of her shorthand notes so taken as

11 aforesaid and contains the proceedings given at

12 said hearing.

13

14

15

Certified Shorthand Reporter

16

17

18

19

20

21

22

23

24

Exhibit F

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

JUDGE DAVID B. ATKINS

FELIPE BERNAL, individually
and on behalf of others similarly
situated,

Plaintiff,

v.

ADP, LLC,

Defendant.

AUG 23 2019

Circuit Court-1879

No. 2017-CH-12364

Calendar 16

Judge David B. Atkins

MEMORANDUM OPINION AND ORDER

THIS CASE COMING TO BE HEARD on Defendant ADP, LLC's Motion to Dismiss Plaintiff's Complaint Pursuant to 735 ILCS 5/2-615, the court, having considered the briefs submitted and being fully advised in the premises,

HEREBY FINDS AND ORDERS:

Background

Plaintiff, Felipe Bernal, as an employee of Rokit Ranch Productions, Inc. ("Rokit"), was required to use biometric scanning technology to "clock-in" and "clock-out." The biometric technology was provided and serviced by Defendant ADP, LLC. Plaintiff alleges the use of his biometric identifying information during his employment with Rokit was improperly acquired, possessed, and disseminated in violation of sections 740 ILCS 14/15 (a)-(d) of the Biometric Information Privacy Act ("BIPA"). Plaintiff originally brought suit against Rokit for said violations, but he subsequently amended his Complaint to drop all allegations against Rokit and instead claim that Defendant violated BIPA. Defendant now seeks to dismiss all counts.

Standard of Review

A 2-615 motion to dismiss challenges the complaint's legal sufficiency based on facial defects.¹ The court assumes all well-pleaded facts and their reasonable inferences in the complaint as true, viewing the allegations in the light most favorable to the plaintiff.² As Illinois is a fact-pleading jurisdiction, "a plaintiff must allege facts sufficient to bring a claim within a legally recognized cause of action."³ Mere conclusions of law and unsupported conclusory factual allegations are insufficient to survive a 2-615 motion to dismiss.⁴ A 2-615 motion to dismiss does not raise affirmative factual defenses.⁵ "A

¹ *Beacham v. Walker*, 231 Ill. 2d 51, 57 (2008).

² *Alpha School Bus Co. v. Wagner*, 391 Ill. App. 3d 722, 735 (2009).

³ *City of Chicago v. Beretta U.S.A. Corp.*, 213 Ill. 2d 351, 355, (2004).

⁴ *Alpha School Bus*, 391 Ill. App. 3d at 736.

motion to dismiss should be granted only if the plaintiff can prove no set of facts to support the cause of action asserted.”⁶

Discussion

Count I of Plaintiff's Complaint alleges violations of four separate clauses within BIPA. The Court addresses each alleged violation separately.⁷

Applicability of § 15(b).

Plaintiff asserts that Defendant violated § 15(b), which imposes certain preconditions that private entities must comply with before they can “collect, capture, purchase, receive through trade, or otherwise obtain” an individual's biometric information. Defendant presents a compelling argument that § 15(b) should not apply to an entity like ADP, pointing out that language included by the legislature differs from the language included in the other subsections and suggests that the legislature intended for possession alone to not be enough to make an entity subject to § 15(b). Indeed, § 15(b)'s requirement that the private entity whose actions the subsection is meant to regulate must receive a “written release” from the subject of the biometric identifier or biometric information or their legally-authorized representative does suggest that the legislature did not intend for the subsection to apply to a third party entity as Defendant seems to be here.⁸ Here, Defendant is not Plaintiff's employer. While Plaintiff correctly contends that BIPA can be applied outside of an employment situation, there is nothing to suggest that BIPA was intended to apply to situations wherein the parties are without any direct relationship.⁹ Moreover, from the facts as they are alleged, the Court can infer that this case fits squarely within an employment context. All of Plaintiff's claims stem from Rockit's requirement that employees participate in biometric scanning technology. That Rockit obtained the technology from Defendant does not remove Plaintiff's case from existing within the context of his employment by Rockit. As Defendant notes, to read BIPA as requiring that a third party provider of the biometric timeclock technology, without any direct relationship with its customers' employees, obtain written releases

⁵ *Borowiec v. Gateway 2000, Inc.*, 209 Ill. 2d 376, 382 (2004).

⁶ *Kaiser v. Fleming*, 315 Ill. App. 3d 921, 925, (2000).

⁷ In his response to Defendant's motion to dismiss, Plaintiff represents that he “voluntarily dismisses his negligence claim (Count II) against Defendant,” thus rendering as moot Defendant's motion to dismiss Count II.

⁸ As Defendant notes in its motion, the BIPA's definition of “written release” clearly limits its applicability, in the context of employment, to the relationship that exists between employer and employee. 740 ILCS 14/10.

⁹ In *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186 (2019), the Supreme Court noted that the purpose of § 15(b) is to vest “in individuals and customers the right to control their biometric information without requiring notice before collection and giving them the power to say no by withholding consent.” 2019 IL 123186 at ¶34. Given the Supreme Court's interpretation of § 15(b)'s purpose, there is little reason to believe that its applicability should extend beyond the point at which an individual has the right to withhold consent. Here, Plaintiff's right to withhold consent can be exercised by refusing Rockit's authority to collect his biometric information.

from said employees would be unquestionably not only inconvenient but arguably absurd.¹⁰

Yet, based on the pleadings, as written, the Court's decision must ultimately turn on the insufficiency of Plaintiff's Complaint as to § 15(b). Plaintiff has failed to allege facts sufficient enough for the Court to properly assess Defendant's actual involvement, relative to the biometric scanning technology, beyond the fact that Defendant supplied Rockit with the technology. In order for the Court to determine whether or not § 15(b) is applicable here, Plaintiff's Complaint must include factual allegations of what Defendant's role relative to Plaintiff's biometric information is. Most of Plaintiff's claims that are relevant to § 15(b) are aimed at what the technology Defendant provides to Rockit allegedly does. In so far that Plaintiff's claims allege particular action on Defendant's part, the allegations are conclusive in nature.¹¹ Therefore, Defendant's motion to dismiss, as to the portion of Count I alleging a violation of § 15(b) of BIPA is GRANTED.

Whether § 15(a) is Moot.

Plaintiff alleges a breach of § 15(a), which requires private entities in possession of biometric information to:

“develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers ... when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric information must comply with its established retention scheduled and destruction guidelines.”

The language in § 15(a) seems to make clear that a private entity is required to comply with its established retention schedule and destruction guidelines whenever in possession of biometric information. The subsection seems to stipulate that the schedule and guidelines must be written and made available to the public. Therefore, if a private entity is in possession of biometric information, but lacks an established retention schedule and destruction guidelines, it stands to reason that said private entity could be found to be in violation of § 15(a).

Notwithstanding the requirement that a private entity in possession of biometric information have an established retention schedule and destruction guidelines, there is no explicit requirement that the schedule or guidelines exist “prior to” possession of the

¹⁰ “It is a familiar rule, that a thing may be within the letter of the statute and yet not within the statute, because not within its spirit, nor within the intention of its makers.” *People v. Hanna*, 207 Ill. 2d 486, 498 (2003) (citing *Croissant v. Joliet Park Dist.*, 141 Ill. 3d 449, 455 (1990) (“Statutes are to be construed in a manner that avoids absurd or unjust results”)).

¹¹ See Plaintiff's Complaint at ¶ 3 (“Defendant ADP is capturing, storing, using, and/or disseminating the biometrics of Plaintiff ...”)

biometrics information. Yet, regarding § 15(a), Plaintiff alleges that “[p]rior to taking Plaintiff’s biometrics, Defendant did not make publicly available any written policy as to a biometric retention schedule and guidelines for permanently destroying the collected biometrics.” While this may be true, such an allegation does not exclude the possibility that Defendant made available to the public an established schedule and guidelines when, and not before, it was in possession of Plaintiff’s biometric information. Plaintiff’s Complaint, as written, does not sufficiently allege an actual violation of § 15(a), and thus, fails to state a claim. Defendant’s motion to dismiss, as to the portion of Count I asserting a violation of § 15(a) of BIPA is GRANTED.

Whether Plaintiff has Sufficiently Alleged a Violation of § 15(c).

Plaintiff alleges an infraction of § 15(c), which prohibits private entities from selling, leasing, trading, or otherwise profiting from an individual’s biometric information.¹² Here, Plaintiff contends that the allegations in his Complaint, “when combined with reasonable inferences that can be drawn therefrom, establish that Defendant obtains and stores the biometric information captured by its devices, which it in turn sells, leases, or otherwise makes commercially available to Plaintiff’s employer for the purposes of biometric timekeeping.”¹³ The court disagrees. Paragraphs 11 and 26 of Plaintiff’s Complaint allege that Defendant disseminates biometric information to “third parties, including vendors for timekeeping, data storage, and payroll purposes.” Plaintiff’s Complaint does not contain any allegation that Defendant sold, leased, traded, or otherwise profited from anyone’s biometric information. Thus, since Plaintiff’s Complaint only alleges facts sufficient to demonstrate that Defendant passes biometric data to third party partners for purposes other than profit, Defendant’s motion to dismiss as to the portion of Count I asserting a violation of § 15(c) is GRANTED.

Whether Plaintiff has Sufficiently Alleged a Violation of § 15(d).

Defendant provides a compelling argument regarding whether § 15(d) is even applicable in this case. Namely, that Plaintiff’s implication of Defendant’s allowing biometric information to pass to data storage vendors and payroll services does not qualify as instances of “disclosure” or “dissemination” under BIPA, but rather should be considered a form of mere transmission. However, to the extent that Defendant’s argument seems to suggest an affirmative factual defense, it would be inappropriate for the Court to entertain this line of argument on a Section 2-615 motion to dismiss.

Turning to the Complaint as pled, Plaintiff asserts a violation of § 15(d), which establishes certain preconditions with which private entities must comply before they “disclose, redisclose, or otherwise disseminate a person’s or a customer’s biometric ... information.” Only twice in Plaintiff’s Complaint does he allege any such disclosure; each instance consists of a single statement that Defendant’s technology “allows for and resulted in” the dissemination of Plaintiff’s biometric information to third parties,

¹² See 740 ILCS 14/15(c).

¹³ See Plaintiff’s response to Defendant’s motion to dismiss at pg. 8.

including vendors for timekeeping, data storage, and payroll purposes.”¹⁴ These allegations fall short of sufficient factual pleading, because they are void of any facts to support Plaintiff’s allegation that Defendant has violated § 15(d). Suggesting that the technology Defendant created allows for the dissemination of biometric information is not an allegation of the Defendant’s disseminating biometric information. Thus, Defendant’s motion to dismiss, as to the portion of Count I asserting a violation of § 15(d) is GRANTED.

WHEREFORE the Court enters an order as follows:

- a. Defendant ADP, LLC’s motion to dismiss Plaintiff Felipe Bernal’s Complaint is GRANTED, and Count I is dismissed *without prejudice*.
- b. Plaintiff has until September 20, 2019 to file an amended complaint, with facts consistent with this Order.
- c. This matter is set for further status to October 24, 2019 at 10:30 a.m. in courtroom 2102.

JUDGE DAVID B. ATKINS
ENTERED:

AUG 23 2019

Circuit Court-1879

Judge David B. Atkins

The Court.

¹⁴ See Plaintiff’s response to Defendant’s motion to dismiss at ¶¶11, 26.